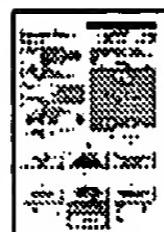


Delphion

Intellectual Property Network

[To Search & Research](#)[IPN Home](#) | [Search](#) | [Order](#) | [Shopping Cart](#) | [Login](#) | [Site Map](#) | [Help](#)Order
plaques
now

S5428606: Digital information commodities exchange

[View Images \(10 pages\)](#) | [Expand Details](#) | [View Cart](#) | [View INPADOC only](#)

Add to cart: [PDF \(~950 KB\)](#) | [TIFF](#) | [Fax](#) | [SmartPatent](#) | [File History](#) |
[More choices...](#)

Inventor(s):**Moskowitz; Scott A.**, Tokyo 158, Japan**Applicant(s):****none****Issued/Filed Dates:****June 27, 1995 / June 30, 1993****Application Number:****US1993000083593****IPC Class:****H04L 12/56;****ECLA Code:****H04L12/58; H04L29/06; H04M3/493;****Class:****Current: 370/400;****Original: 370/060; 370/094.1;****Field of Search:****370/60,60.1,85.1,32,53,54,58.1,58.2 358/85,86 379/61,110,219,220 348/7,10,12****Legal Status:**

Gazette date	Code	Description (remarks) List all possible codes for US
Oct. 19, 1999	PRDP	Patent reinstated due to the acceptance of a late maintenance fee (990827)
Sept. 21, 1999	FP	Expired due to failure to pay maintenance fee (19990627)
June 1, 1999	AS02	Assignment of assignor's interest (WISTARIA TRADING, INC #2505 16771 COLLINS AVENUE MIAMI, FLORIDA 33160 * DICE COMPANY : 19990512)
Dec. 27, 1996	AS02	Assignment of assignor's interest (DICE COMPANY, THE P.O. BOX 60471 PALO ALTO, CALIFORNIA 94306-047 * MOSKOWITZ, SCOTT A. : 19961212)
June 27, 1995	A	Patent
June 30, 1993	AE	Application data

Abstract:

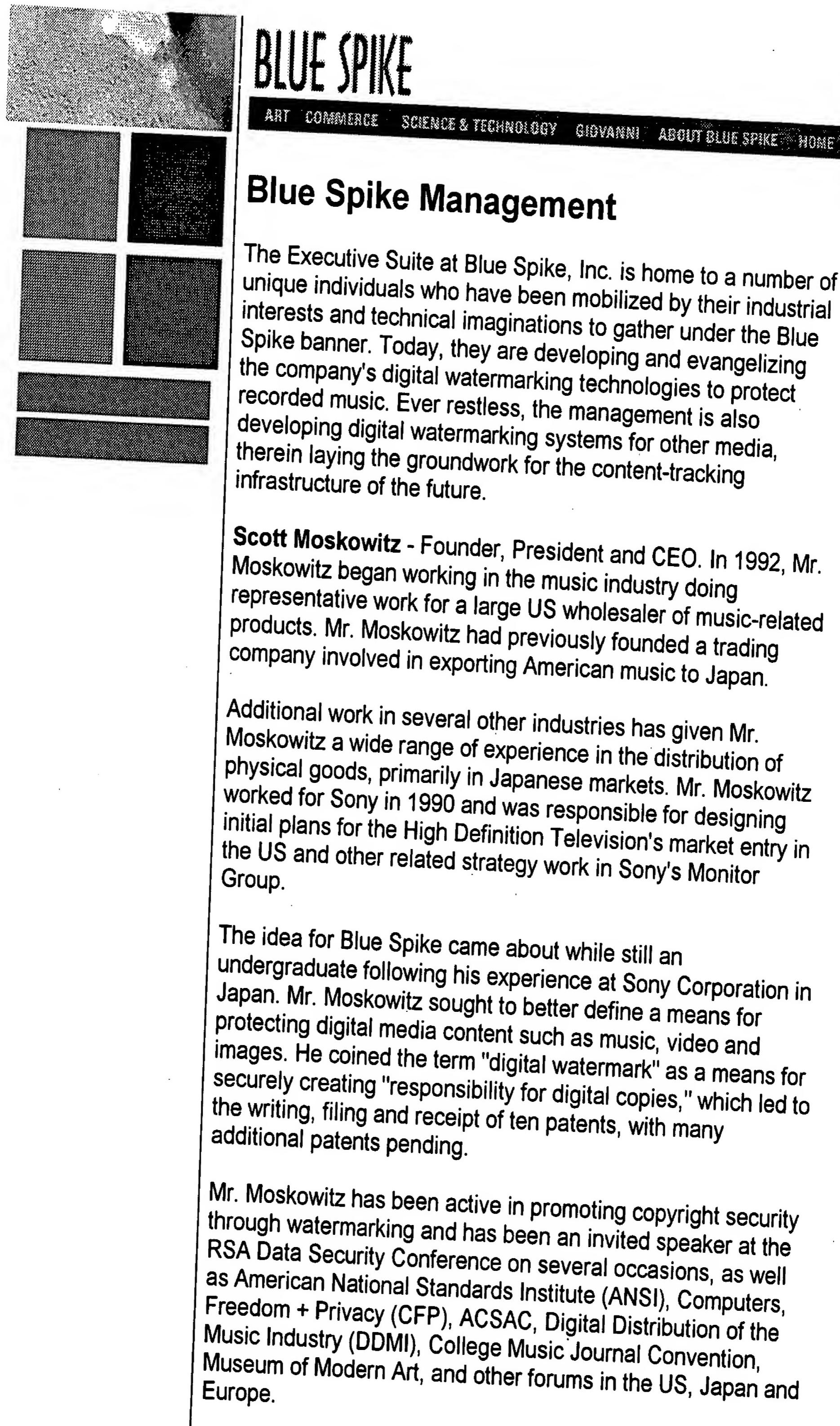
A system for the exchange of digital information packets includes an exchange with connectors to allow modular expandable units to connect to the exchange over transmission media. The modular expandable units send digital information packets from one to another over the exchange in response to requests for these digital information packets. The exchange allows for billing and other administrative functions.

In effect, Moskowitz was hiding his title to the CDs in plain sight. That concept has been most fully developed in the mathematical craft of steganography, a subset of cryptography but, in actuality, the earliest form of this mathematical discipline. (It was used by ancient Chinese and Greek armies to obscure military intelligence. From the Greek, it roughly translates into covered-up writing.) Moskowitz became a fast and dedicated student of the steganographic arts and fused it with his understanding of finance and retail market-making - hard-earned knowledge acquired in corporate and entrepreneurial forays in the US and Japan.

In 1995, Moskowitz filed his very first patents relating to digital watermarking, at the time little more than an academic curiosity with maybe a handful of practitioners who understood what it meant and the applications it could actuate. Today, Blue Spike stands astride an estate of more than a dozen patents related to digital watermarking, it is marketing software that animates the patented innovations, and it is leading industrial discussions on the development of digital watermarking standards for protecting recorded music.

Suddenly, though actually after years of slogging patents and hammering code, Blue Spike has found itself at the nexus of one of the pivotal technologies of the information age, one that will provide the labelling and tagging that is necessary for online commerce to operate as efficiently as its offline cohort - and to enjoy some of the unique efficiencies of the digital marketplace. Industry groups are developing standards for digital watermarking; captains of industry are calling for Congress to require that players be equipped to read digital watermarks to control illegal copying; and, no surprise, digital watermarking is regularly discussed in newspapers as well as trade and business magazines.

In retrospect, it seems that Michelle's act of policing was both inspirational - and prescient. As she recognized Moskowitz's personal mark to establish responsibility for his drafting instrument, Blue Spike's digital watermarking is going to be the marking scheme by which the universe of digital objects will be assigned to their rightful owners and copyright holders. Whither the Muse? Occasionally, Moskowitz will bump into her in the neighborhood. Still funny. Still protective. "If she caught anyone with my stuff stolen today - she would do the same thing now as she did then," Moskowitz says.



The Blue Spike website features a dark header with the company name in large, white, sans-serif letters. Below the header is a navigation bar with links to ART, COMMERCE, SCIENCE & TECHNOLOGY, GIOVANNI, ABOUT BLUE SPIKE, and HOME. The main content area contains several sections of text and images. On the left side, there is a vertical column of five black rectangular boxes of varying sizes, some with a fine dot pattern. The first section of text discusses the company's management suite and their focus on digital watermarking technologies. The second section, under the heading 'Scott Moskowitz - Founder, President and CEO', provides a detailed biography of Mr. Moskowitz's background in the music industry, including his work at Sony. The third section describes how the idea for Blue Spike originated from Mr. Moskowitz's experience at Sony Corporation in Japan. The fourth section highlights Mr. Moskowitz's active role in promoting copyright security through speaking at various conferences and forums.

BLUE SPIKE

ART COMMERCE SCIENCE & TECHNOLOGY GIOVANNI ABOUT BLUE SPIKE HOME

Blue Spike Management

The Executive Suite at Blue Spike, Inc. is home to a number of unique individuals who have been mobilized by their industrial interests and technical imaginations to gather under the Blue Spike banner. Today, they are developing and evangelizing the company's digital watermarking technologies to protect recorded music. Ever restless, the management is also developing digital watermarking systems for other media, therein laying the groundwork for the content-tracking infrastructure of the future.

Scott Moskowitz - Founder, President and CEO. In 1992, Mr. Moskowitz began working in the music industry doing representative work for a large US wholesaler of music-related products. Mr. Moskowitz had previously founded a trading company involved in exporting American music to Japan.

Additional work in several other industries has given Mr. Moskowitz a wide range of experience in the distribution of physical goods, primarily in Japanese markets. Mr. Moskowitz worked for Sony in 1990 and was responsible for designing initial plans for the High Definition Television's market entry in the US and other related strategy work in Sony's Monitor Group.

The idea for Blue Spike came about while still an undergraduate following his experience at Sony Corporation in Japan. Mr. Moskowitz sought to better define a means for protecting digital media content such as music, video and images. He coined the term "digital watermark" as a means for securely creating "responsibility for digital copies," which led to the writing, filing and receipt of ten patents, with many additional patents pending.

Mr. Moskowitz has been active in promoting copyright security through watermarking and has been an invited speaker at the RSA Data Security Conference on several occasions, as well as American National Standards Institute (ANSI), Computers, Freedom + Privacy (CFP), ACSAC, Digital Distribution of the Music Industry (DDMI), College Music Journal Convention, Museum of Modern Art, and other forums in the US, Japan and Europe.

He is the author of "So this is Convergence?" recently published in Japan, the only book of its kind on secure digital watermarking. Mr. Moskowitz earned his Bachelor of Science degree in Economics, cum laude, with a concentration in Finance, from The Wharton School, and a Bachelor of Arts degree, cum laude, in Political Science and Oriental Studies, from the University of Pennsylvania. Mr. Moskowitz is fluent in spoken and written Japanese and spent seven years as a resident of Tokyo. He is a member of the Institute of Electrical and Electronics Engineers (IEEE), Association for Computing Machinery (ACM) and The International Society for Optical Engineering (SPIE) organizations.

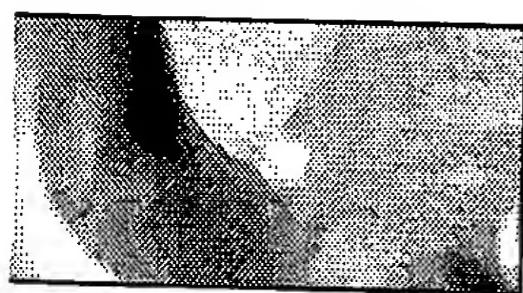
Gregg Moskowitz - Vice President, Business Development. Prior to joining Blue Spike in January of 1999, Mr. Moskowitz founded a company that provided individuals the ability to consummate consumer-to-consumer transactions with their credit cards. The purpose of this novel concept is to give consumers an additional medium for buying and selling used merchandise. Previously, Mr. Moskowitz was a Senior Associate in the business turnaround and corporate restructure division with Price Waterhouse. His diverse experience at Price Waterhouse ranged from the restructuring of distressed companies to providing financial and operational advisory services to Fortune 500 companies. Mr. Moskowitz graduated from the University of Wisconsin-Madison in 1993 with a BS degree in Accounting and Risk Management and Insurance. Mr. Moskowitz is a Certified Public Accountant.

Mike Berry - Chief Technology Officer. Mr. Berry is a computer programmer specializing in audio and image signal processing. Mr. Berry leads Blue Spike's development of the Giovanni digital watermark system as chief engineer for the Company, and has created all of the core technology implementations for the Company over the past 3 years. He studied Music Composition at Amherst College and Mills College. He is the author of the award-winning software synthesizer GrainWave and the software effects processor Pedalfects. He has also written audio signal processing code for Mixman, Prosoniq, and Opcode.

Peter Cassidy - Director of Marketing and Communications. Mr. Cassidy is a widely published writer, analyst, business development consultant, speaker and a co-founder of the Digital Commerce Society of Boston. Mr. Cassidy has authored articles and opinion columns under his own byline for international business publications such as The Economist, ForbesASAP and WIRED as well as dozens of publications worldwide. His reporting on national political affairs has been reprinted in text books and anthologies. He has also

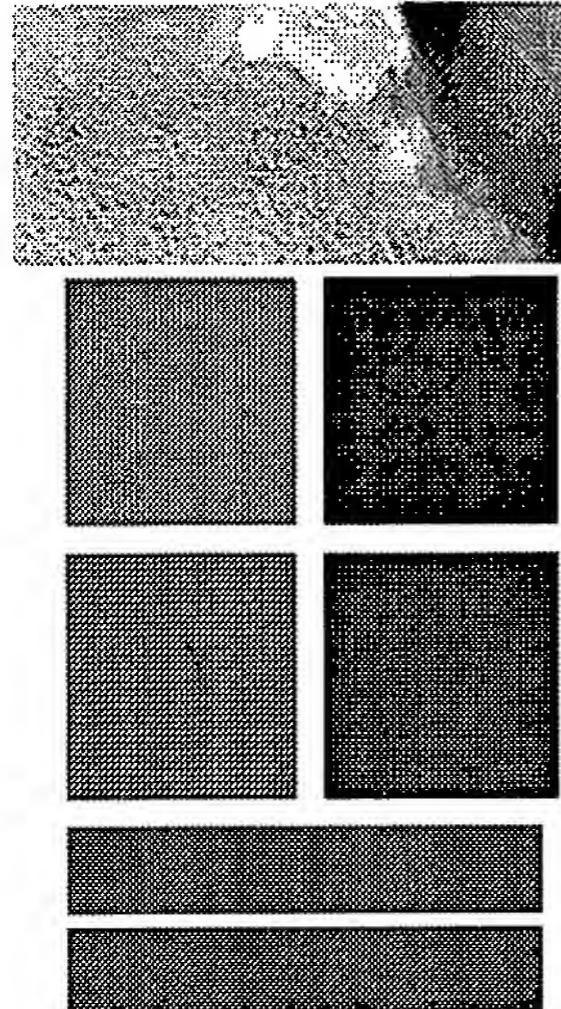
contracted as a consultant to syndicated television magazine programs in the United States and Britain. As a business consultant, he has assisted in the development of many security related products and services (among them license management systems, digital receipting schemes and network security auditing services), in the formation of marketing communications plans, and in the development of marketing communications instruments. Among the companies that have engaged him or consumed his analyses have been: Banyan, Aladdin Knowledge Systems, Isogon, Lotus, NTT, GTE, and Receipt.com (now a division of Valicert), Cylink and Compaq. Mr. Cassidy has been invited to speak at industry conferences and colloquia in Boston, Sao Paulo and San Diego commenting on distance learning technologies, payment systems, cryptographic export controls, software license management, on-line privacy and the evolution of intellectual property control systems for commerce on the Internet.

Hitoshi Sakamoto - Director of Blue Spike Japan. After graduating Senshu University in Tokyo majoring in Commerce and Canon's International Business School in Hawaii majoring in Computer Science, Mr. Sakamoto joined Three One Systems, Inc. & Design Technologies, Inc. He spent 10 years there as a member of the Board of Directors responsible for Fractal Image Compression technology. In 1996, he established Cedge Ltd. in Tokyo as president, which is a consulting company of multimedia technologies, such as digital watermarking and image compression. Mr. Sakamoto was responsible for the Japanese translation of the Blue Spike web site and the translation and publication of the first book on secure digital watermark: "So this is Convergence?" Born in 1958, Mr. Sakamoto has worked with Blue Spike promoting and marketing the Company's technology since its inception.



EMAIL CONTACT

Copyright © 2000 Blue Spike, Inc. All rights reserved.
Send comments and suggestions to webmaster@bluespike.com



BLUE SPIKE

[ART](#) : [COMMERCE](#) : [SCIENCE & TECHNOLOGY](#) : [GIOVANNI](#) : [ABOUT BLUE SPIKE](#)

Innovations in Digital Copyright Protection

For those who create, produce, distribute, promote, package and consume digital artwork and music, digital distribution need no longer be tantamount to surrendering your treasures to information highway bandits. With Blue Spike's watermarking technologies, your content can all but phone home. Explore the power of securing electronic content through digital watermarking in the following site segments:

Art

Come see the show at Blue Spike's Future Think Studio, a gallery and a laboratory in which digital art is at last indelibly signed by the artist. And get the inside dope on Metallica's struggle with online piracy.

[\[More\]](#)

Commerce

Online commerce lurches forward in a terrifyingly haphazard and inordinate fashion. Today "e-commerce" might as well stand for "entropy commerce." On the way are the e-labels, e-tags, e-money, e-receipts and e-boxes that will automate online business functions.

[\[More\]](#)

Science & Technology

For users of our Giovanni watermarking system, copyright security is a point-and-click affair. Beneath Giovanni's elegant interface, however, lie intricate orchestrations of psycho-acoustic modeling techniques and the mathematics of cryptography. [\[More\]](#)

Giovanni

Giovanni digital watermarking systems give creators and distributors penetrating control over their digital properties - and they can enable online distribution schemes otherwise unthinkable without prohibitively complex technologies. [\[More\]](#)

About Blue Spike

Look in here for more about our company, its technologies, its intellectual and business provenance, its philosophies, its management team and the exciting news it is generating. [\[More\]](#)

Manifesto: So This is Convergence?

Blue Spike's founder considers the consequences of virtually unlimited distribution capacity being set upon the world today through the Internet - and the role of digital watermarking in bringing technical, legal and commercial order to this penetrating new medium.

Download it here in PDF format: [\[More\]](#)

Show me the Patents

US Patent #5,905,800 Method and System for Digital Watermarking, US Patent #5,822,432 Method for human-assisted random key generation and application for digital watermark system, US Patent #5,745,569 Method for Stega-cipher Protection of Computer Code, US Patent# 5,687,236 Steganographic Method and Device, US Patent# 5,613,004 Steganographic Method and Device, US Patent# 5,539,735 Digital Information Commodities Exchange, US Patent# 5,428,606 Digital Information Information Commodities Exchange

For information, contact: info@digital-watermark.com

Interesting Links

- [Giovanni Media Security](#)
 - [Watermarking, Steganography & Information Hiding - Fabien Petitcolas](#)
 - [Watermarking Links - Deepa Kundur](#)
 - [WWW References on Multimedia Watermarking and Data Hiding Research & Technology - Frank Hartung](#)
 - [Alessandro Piva - Digital Watermarking](#)
-

Copyright © 1999 Scott Moskowitz



[Search Lucent](#) [GO >](#) [Advanced Search >](#)

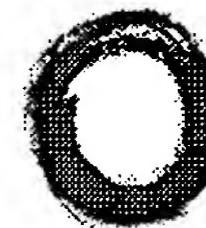
[news & info](#) [solutions](#) [international](#) [careers](#) [bell labs](#) [site info](#)

>> press room > press releases > press archive > investor relations > corporate info

news & investor info

press release

Lucent Technologies
Bell Labs Innovations



Lucent Technologies and Blue Spike announce alliance for digital music security

FOR RELEASE MONDAY JANUARY 24, 2000

MIDDLETOWN, N.J. and MIAMI, FL. - Lucent Technologies (NYSE: LU) and Blue Spike, Inc., a leading developer of secure digital watermarking applications that enable copyrights to be embedded into audio or video content, today announced an alliance that will incorporate the Lucent Enhanced Perceptual Audio Coder™ (ePAC™), the industry's leading audio coder, into Blue Spike's leading-edge music security solution.

The ePAC coder will be integrated into Blue Spike's "end-to-end" solution for music security, which enables producers to offer piracy-proof music products with the highest audio quality for both electronic delivery and packaged media. Music packages embedded with the Blue Spike digital watermarking solution can now gain CD-quality sound with ePAC while maintaining the integrity of the original source material, even when mixed with enhanced text, images, and video. The scaleable system can be used on a wide range of products, including portable music players, personal computers and high-end stereo equipment.

"The Blue Spike end-to-end solution, combined with ePAC, is an ideal product for the secure digital music industry, enabling greater degrees of copyright protection across the industry," said Joyce Eastman, director of audio initiatives for Lucent Technologies. "The elegance of Blue Spike's product, with its 'trusted transactions' technology, helps assure producers that they can encode with ePAC and deliver their content, fully protected, across a range of digital media platforms."

Both Lucent Technologies and Blue Spike are members of the Secure Digital Music Initiative (SDMI), the worldwide recording industry's effort to develop an open, secure access system for digital music.

"Lucent provides us with an exceptional audio compression package that allows us to demonstrate a complete solution for music copyright owners," said Scott Moskowitz, president of Blue Spike. "We believe that this is the answer to the music industry's digital copyright problem."

Blue Spike and Lucent are natural partners to offer a secure state-of-the-art electronic music distribution system. Lucent is a pioneer in high quality audio compression and Blue Spike is a pioneer in digital watermarking. When combined with security technologies, the combination of Lucent's ePAC and Blue Spike's watermarking will provide an ideal solution for Internet delivery of music, ensuring high quality and a pleasurable experience for consumers while protecting the rights of copyright owners.

Lucent's ePAC coder is interoperable with RealNetworks' G2 Player and has been licensed to e.Digital for its handheld Internet music device and to Lydstrom, Inc. for its Songbank home Internet stereo device. The ePAC coder will also be integrated into VedaLabs' music software and hardware platforms.

ePAC is based on the Lucent Perceptual Audio Coder™ (PAC™), the highest-quality digital audio codec in the industry.

ePAC is a new version of the Lucent Perceptual Audio Coder™ (PAC™) developed by Bell Labs, the research and development arm of Lucent Technologies. PAC is an audio compression algorithm with the highest-quality audio at the lowest bit rates. At 128 kilobits per second, ePAC offers CD-transparent stereo sound.

ePAC uses psychoacoustic modeling - that is, a representation of how humans hear sound - to compress music in a way that is not noticeable to the ear. Music is compressed at a rate of 11 to 1, thus reducing the transmission time/bandwidth and storage by the same ratio, while still retaining its fidelity.

Several recent improvements in ePAC have pushed its performance levels to new heights, including: ePAC's improved quantization and coding, allowing higher quality audio at lower bit rates, and ePAC's improved psychoacoustic modeling from Bell Labs research, which provides CD-transparent sound at 128 kbps.

ePAC's variable bit rates and superior audio quality allow the coder to be used in multiple bandwidth applications.

Lucent Technologies' famed research and development arm, Bell Labs, has been at the forefront of technology for the music industry for decades, with the introduction of sound for motion pictures in 1926; the invention of stereo recording in 1933; the invention of the transistor in 1947; the introduction of computer-synthesized music in the 1950s; the introduction of psychoacoustics in the 1960s; sub-band coding of audio in the 1970s; the introduction of linear predictive coding in the 1980s, and the Perceptual Audio Coder in the 1990s.

Blue Spike is the leading provider of secure digital watermarking and content protection technologies based on an extensive patent portfolio. Blue Spike's technology enables owners of multimedia content such as music labels, movie studios, banking and financial institutions and government agencies to establish ownership over digital copies, and to identify legitimacy of digital information that otherwise would appear to be exact, perfect copies. Blue Spike's digital watermarking application is the only provably secure watermarking system that makes use of cryptographic keys, which are used to authenticate the digital asset. Blue Spike's "trusted transactions" represent a new era for bridging cryptographic security with human trust. Trusted transactions are a leading contender for democratizing security for all transactions. For more information on Blue Spike's technology visit the company's Web site at <http://www.bluespike.com/>.

Lucent Technologies, headquartered in Murray Hill, N.J., designs, builds and delivers a wide range of public and private networks, communications systems and software, data networking systems, business telephone systems and microelectronic components. Bell Labs is the research and development arm for the company. For more information on Lucent Technologies, visit the company's Web site at <http://www.lucent.com>.

For more information, reporters may contact:

Chris Pfaff
Lucent Technologies
908-582-7571 (office)
800-705-2368 (pager)
Email:cpfaff@lucent.com

Wendy Zajack
Lucent Technologies
908-582-4824 (office)
Email:wzajack@lucent.com

Gregg Moskowitz
Blue Spike, Inc.
212-725-3974 (office)
Email:gregg@bluespike.com

[Lucent Home](#) | [Service Provider](#) | [Enterprise](#) | [Avaya](#) | [Small to Mid Business](#) | [OEM](#) | [Business Partner](#) | [US Government](#) | [Investor](#)

Copyright © 2000 Lucent Technologies. Use of this site indicates you accept the Terms of Use and the Privacy Statement. For comments or questions about this site, contact us.

THE MAIL ARCHIVE

cryptography

[<- Chronological -->](#)Find [<- Thread -->](#)

Re: Blue Spike and Digital Watermarking with Giovanni

-
- From: Eugene Leitl
 - Subject: Re: Blue Spike and Digital Watermarking with Giovanni
 - Date: Sun, 16 Jan 2000 10:27:09 -0800
-

Robin Whittle writes:

> Digital watermarks again!
>
> Joe Sixpack won't believe his file contains a digital watermark with
> his name in it unless there is a freely distributed Windows/Mac
> program which reads the watermark and so spits out his name and other
> personal details.

Joe Sixpack also doesn't believe that color laser copiers leave an unique signature on each copy, allowing you to trace the copy to an individual device. Nevertheless these are there, and can be evaluated if need arises. (Just try distributing a few xeroxed \$100 bills, and time how long it takes until the feds knock on your door).

> That being the case, it is only a matter of time before the code and
> the watermark algorithm is reverse-engineered. Then a program can be
> written to remove the watermark.

The algorithm will be kept secret, of course. Watermarking is not content, and hence need not to be presented to the end consumer. Thus Achilles' heel of content encryption which must be decoded into the (almost always interceptible) plain by some enduser-gadget-resident algorithm is avoided.

> What use is the watermark anyway? It is only applicable to files
> generated for a specific, legally identifiable customer. Therefore it
> does not apply to pre-pressed CD/DVD etc. discs or to broadcasts via
> the Net, TV, radio etc.

There is clearly a trend for point-to-point, individual content distribution. With the proper infrastructure it should be possible to insert watermarks even in realtime "broadcast" content (which is mostly news and hence grows stale real quick).

> Who is going to prosecute Joe Sixpack or Jo Lipstick? Not a big
> company which is interested in its public image. Not a small company,

Well, it's a tree, starting with Joe Sixpack as a root. While "six

"degrees of separation" is a cliche, the amplification at each step can be considerable. Construed (=purely arithmetical) damage can be considerable.

> because of the the costs. Maybe a big company which doesn't care
> about its reputation - to set and example. But that would only
> encourage all the other Joes and Jos to copy some more!

The problem does exist. See <http://napster.com/> and
<http://www.mp3.com/news/471.html>

It may not be properly addressed today, but it's there.

> What's the use when Joe or Joe's watermarked, or proprietary-encoded
> audio file must be reproduced via a PC soundcard, and there are
> programs to write the raw 16 bit data to disk as .WAV or perhaps as
> .MP3? I guess the same principle applies to video.

Broadband encoded watermarks should survive multiple digital-analog-digital conversions. Remember, all we have is to hide a few 10 bits in a multi-MBytes/GByte stream. You don't know what are bits and what is noise.

> (Linear media such as text, audio and video cannot be copy-protected.

ASCII? You can encode information in formatting, interpunction, alternative spelling. A diff between two text versions will readily reveal sneakiness, but automatically stripping such information without losing content is nontrivial. Audio and video can most assuredly be watermarked, the question is how resistant to stripping/mangling these watermarks will turn out to be.

> Material constituting computer software - something interactive which
> must run on a CPU and do things with a user - can be protected
> reasonably well via hardware keys or better still, live links to a

Cracking dumb dongles is semitrivial. Crypto dongles are harder, of course. But the code must still be executed in plain (until crypto is handled within the CPU), and is thus vulnerable.

> server via the Net. The security of such transactions would be a
> worry for network administrators . . . and anyway, watermarking is
> only for linear media.)

Define linear media. Everything is reducible to a bitstream.

> If the watermark is inaudible, then why should we believe it will
> survive compression schemes which cut to the bone of human perception?

Because storage is cheap and compression algorithms are imperfect.

> If it is audible, then why would anyone want to buy the watermarked
material? Considering the bizarre beliefs in so-called "high-end"

I wouldn't buy it whether audible or not. Provided I know that medium is watermarked, which might not be exactly widely advertised. See color xerox machines.

> hi-fi (which resemble religiously inspired fear and fervor - such as
> so-called clock jitter in SP/DIF electrical/optical cables,
> oxygen-free copper power cords . . .) then why would this segment of
> the market accept deliberately altered goods, especially when they
> can't hear it but *know* it's there?

Digital media people high-end audiophiliacs are not. I'm not playing

my mp3's via an external digital input amplifier either (but I wish I could).

> Both the Internet and CD-Rs put mass digital copying in the hands of
> consumers. Content creators need to make the most of this, not fool

Burning CDRs takes time and ties up equipment. Hard drives and xDSL allow sufficiently easy and fast (or in the background) copying.

> themselves they can prevent it. They need to build positive, trusting
> relationships with people who might be prepared to purchase their
> material. There is no alternative. Building these kinds of

I agree. However, they might still put up a considerable fight.

> relationships would be very difficult with the old pre-pressed disc
> (or cylinder in the century before last) paradigm which constitutes
> the established record industry. Those are mass-market, time-delayed
> capital- transport- and labour-intensive approaches - but worst of all
> they are one-way.

I hear you, but the world has inertia. I would also love to pay artists directly with digicash in realtime. We're not exactly there yet.

> Fortunately, the Net is the ideal basis for building these lasting,
> happy relationships.
>
> To continue this line of discussion, with diagrams, see something I
> wrote in 1995, which is still largely relevant: Music Marketing in
> the Age of Electronic Delivery:
>
> <http://www.firstpr.com.au/musicmar/>

Thanks for the pointer.

- Follow-Ups:

- **Re: Blue Spike and Digital Watermarking with Giovanni**

- *From: bram <01/16/2000>*

- **Re: Blue Spike and Digital Watermarking with Giovanni**

- *From: Robin Whittle <01/16/2000>*

- References:

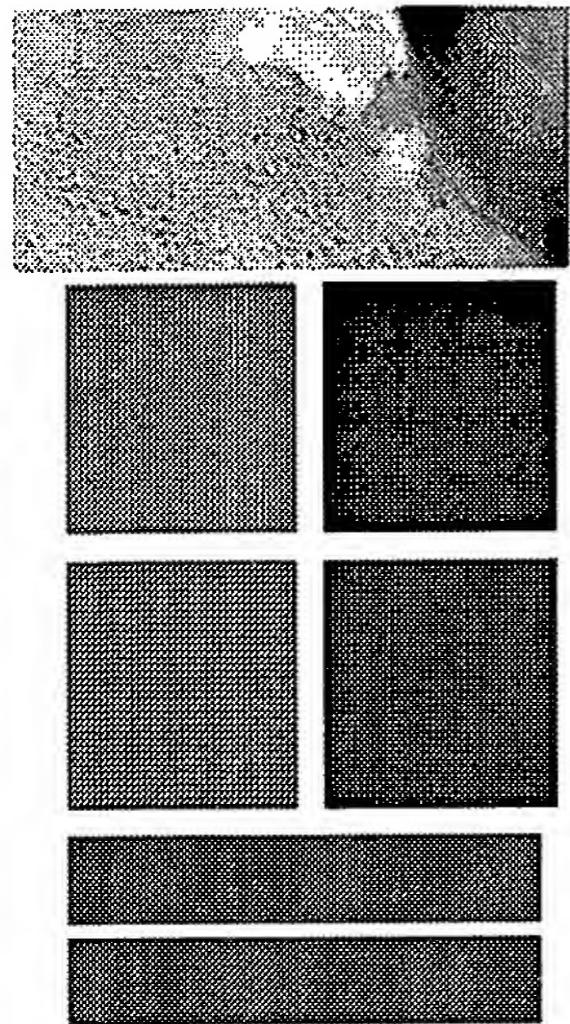
- **Blue Spike and Digital Watermarking with Giovanni**

- *From: Kevin Milani <01/14/2000>*

- **Re: Blue Spike and Digital Watermarking with Giovanni**

- *From: Robin Whittle <01/15/2000>*

- Prev by Date: [Re: Blue Spike and Digital Watermarking with Giovanni](#)
- Next by Date: [Re: Blue Spike and Digital Watermarking with Giovanni](#)
- Prev by thread: [Re: Blue Spike and Digital Watermarking with Giovanni](#) Reply via email to
Eugene Leitl
- Next by thread: [Re: Blue Spike and Digital Watermarking with Giovanni](#)
- Index(es):
 - [Main](#)
 - [Thread](#)



BLUE SPIKE

[ART](#) [COMMERCE](#) [SCIENCE & TECHNOLOGY](#) [GIOVANNI](#) [ABOUT BLUE SPIKE](#) [HOME](#)

Blue Spike In the News Around the World

It's just early days in the development of Blue Spike, but the company's position as the first mover and innovator *sui generis* in digital watermarking technologies is already well evident. Watch this space for the latest news on Blue Spike's commercial coups and provocative industrial commentary as recorded in the trade press. Media representatives with further inquiries may direct them to Blue Spike PR via toll-free phone at 877-815-6039 or e-mail at press@bluespike.com.

Analysis: Bid to secure digital music on the Net hits dissonant chord

MARCH 8, 2000 - In an effort to put its stamp on what is already a burgeoning multimedia market, the Recording Industry Association of America (RIAA) and the world's five major recording companies laid out an ambitious goal this week of creating an umbrella standard for securely sending digital music over the Internet.

Lucent Technologies and Blue Spike announce alliance for digital music security

JANUARY 24, 2000 - Lucent Technologies (NYSE: LU) and Blue Spike, Inc., a leading developer of secure digital watermarking applications that enable copyrights to be embedded into audio or video content, today announced an alliance that will incorporate the Lucent Enhanced Perceptual Audio Coder™ (ePAC™), the industry's leading audio coder, into Blue Spike's leading-edge music security solution.

NTRU and Blue Spike Partner for Digital Music Security

JANUARY 19, 2000 - NTRU Cryptosystems, Inc., a creator of a secure public key cryptography system, and Blue Spike, Inc., the leading developer of secure digital watermarking applications today announced a partnership that will incorporate NTRU's public key encryption technology with Blue Spike's leading-edge "end-to-end" music security solution.

Blue Spike releases their watermarking demo, offering copyright protection

JULY 5, 1999 - Blue Spike, Inc. has worked extensively to ensure that its powerful, patented Giovanni® suite of media security technologies is made available to all. Four years of debates, tests, and initiatives resoundingly conclude that copyright protection is an invaluable element for dramatically expanding the business of music. We strongly believe security must not be shrouded in secrecy.

Digital watermarking showdown between ARIS and Blue Spike

JUNE 3, 1999 - The industry group composed of IBM, Intel, Matsushita Electric and Toshiba, working with record companies on a content-protection framework for DVD-Audio, is expected to pick a digital-watermarking technology at a June 11 meeting.

Aris and Blue Spike pitch their rival watermark technologies

JUNE 17, 1999 - With the so-called 4Cs expected to shortly announce their choice of digital watermarking technology for DVD audio, Aris Technologies Inc. made its case for its MusiCode technology earlier this week, and said the technology will find other markets even if it is not selected by the 4Cs.

Digital Watermarking Takes On Net Music Players

MARCH 15, 1999 - Digital watermarking, a kind of electronic branding of audio and video, is emerging as a must-have technology that could gate the release of music and films for next-generation DVD and Internet consumer-electronics systems.

Watermarking raises cost, control issues

JULY 24, 1998 - Computer and consumer-electronics companies are jockeying to set standards for digital watermarking — a technique for electronically identifying and protecting copyrighted material. The technology they establish could bring a new level of security to digital videodisks and could prove a key enabler for electronic commerce via the Internet, cable TV and satellite.



EMAIL CONTACT

Copyright © 2000 Blue Spike, Inc. All rights reserved.

Send comments and suggestions to webmaster@bluespike.com

**Analysis: Bid to secure digital
music on the Net hits dissonant
chord**

By Margaret Quan
EE Times
(12/18/98, 3:59 p.m. EST)

NEW YORK — In an effort to put its stamp on what is already a burgeoning multimedia market, the Recording Industry Association of America (RIAA) and the world's five major recording companies laid out an ambitious goal this week of creating an umbrella standard for securely sending digital music over the Internet. But the announcement was greeted by concern that the Secure Digital Music Initiative (SDMI) faces an uphill battle in getting a growing group of chip, software and systems suppliers to sing from the same sheet of music.

RIAA president and chief executive officer Hilary Rosen said the group plans to have its first meeting in February and to prepare a specification in time for SDMI-certified products to ship in fall 1999. But even sources who expressed support for SDMI said the schedule is not realistic given the range of existing compression and security options the effort will have to embrace. Among them is MP3 (MPEG 1, Layer 3), a compression scheme for which 5 million to 10 million audio players have already been downloaded from the Web.

"I expect in the next couple of months that we will see players [speak out] from all different sides of the issues," said Richard Doherty, president of the Envisioneering Group consulting firm (Seaford, N.Y.). "Semiconductor companies and others will say they have technologies that they want to be recognized, and will want to take part in the effort."

"I think the assembly at the first meeting will be a lot bigger than RIAA expects," Doherty said. "They could have government agencies looking for some piece of a digital music purchase."

MP3 is the most entrenched of several techniques for compressing or encrypting audio files for Internet audio players. Other approaches include MPEG-2 Advanced Audio Coding, which is being promoted by many consumer electronics companies for satellite TV as well as CD-quality music; Perceptual Audio Coding (PAC), developed by Bell Labs and currently proposed as a U.S. digital radio standard; the so-called "a2b" music services

operated by AT&T; and Liquid Audio, an Internet audio compression and encryption algorithm from the Redwood City, Calif., company of the same name.

In addition, Kobe Steel and Nippon Telegraph and Telephone gave a technology demonstration earlier this year of a portable digital music player dubbed SolidAudio, based on a C5000 series of DSPs from Texas Instruments Inc. It used NTT's Twin VQ compression technology (transform-domain weighted interleave vector quantization) to compress digital music files.

Given the number of players, even SDMI backers say the group's schedule is overly aggressive. "If they intend to have devices out by 1999, that means the devices would have to ship in October, so the specifications would have to be nailed down in March," said Kenneth R. Wirt, vice president of corporate marketing for Diamond Multimedia Systems Inc. (San Jose, Calif.), which is enmeshed in a legal battle with the RIAA over its Rio PMP300 MP3 portable player.

"With the first meeting scheduled for February, it's unlikely it will get done in time, unless they've already got a straw-man proposal they plan to unveil at the first meeting," said Wirt.

Diamond will support the SDMI work, he added, but is also moving ahead with its own plans to support other techniques as well. The company is working on a second-generation Rio player and plans to introduce an application programming interface in early 1999 that will allow companies promoting various encryption schemes to work with Rio. The first API will allow users to download, decrypt, export and play music files based on Liquid Audio files on their Rio players.

Cary Sherman, senior executive vice president and general counsel for RIAA, explained that SDMI's intention is not to choose one digital music technology that will win out over all others, but rather to bring all of the competing technologies to the table. The endgame, Sherman said, will be an open specification with which all of the technologies will interoperate. In fact, RIAA prefers technical competition in the service of innovation, he said.

However, the group was not specific about its stance on various forms of secure transmission, including compression, encryption and digital watermarking.

Clearly, SDMI has big backers, including the heads of BMG Entertainment, EMI Recorded Music, Sony Music Entertainment, Universal Music Group, Warner Bros. and Warner Music Group, the International Federation of the

Phonographic Industry and the Recording Industry Association of Japan.

And the technology companies already on board are something of a who's who of the industry. Among them were America Online, Aris Technologies, AT&T, Creative Technology Ltd., Diamond Multimedia, Headspace Inc., IBM, Iomega, Liquid Audio, Lucent Technologies, Matsushita, Microsoft, RealNetworks, Samsung Electronics, Sony Corp. of America and Texas Instruments.

Other companies are likely to participate via the Copy Protection Technical Working Group (CPTWG), an ad hoc, voluntary industry group that includes representatives and engineers from Hollywood studios, computer and consumer electronics companies. RIAA's Rosen said SDMI will consult with the CPTWG on the specification.

Despite its broad backing the group has raised hackles in the burgeoning Internet audio world. Many in the MP3 community believe the SDMI is RIAA's last attempt to gain control of the digital music industry that has sprung up behind its back and without its blessing. They say the effort is too late, noting for instance that MP3 has already become a de facto standard because it is the only open, ISO spec available for digitally compressed music.

MP3 has gained its following in part because it is free, and both players and music clips in the format are widely available. Other formats are typically proprietary solutions that require either purchase of software or paying a fee to the company that developed them. More than 100 kinds of MP3 players available, according to the MP3 Association. Software support includes Microsoft's Windows 98 and Net Show, Macromedia Shockwave and RealPlayer.

"MP3 will not be going away," said Paul Goldberg, vice president of audio products and intellectual property at Zoran Corp.

A spokesman from Goodnoise (Palo Alto, Calif.), a company that sells MP3 content over the Internet, said the MP3 Association is currently looking at specs for digital signatures and watermarking, but is making no attempt to provide copyright protection.

Meanwhile, the formation of the SDMI appears to have lit a fire under the CPTWG, motivating that group to turn its attention to digital copyright protection issues for audio, not just video. Some suggest audio has been an afterthought for much of the three years the CPTWG has met.

Alan Bell, program director of digital media standards for IBM's Internet Media Group (Cupertino, Calif.) and a CPTWG leader, told EE Times that

the group has discussed the possibility of creating a subgroup to focus on copyright protection issues for digital music. It may go forward with the plan in January, he said.

CPTWG was not part of RIAA's press conference earlier this week, but Bell told EE Times there is considerable interest among CPTWG members to work with the SDMI. He said IBM, Intel and Microsoft have all expressed interest in participating in such a subgroup.

"I think it is very good idea for SDMI and CPTWG to work together, and I expect and hope there will be a relationship between the two," Bell said. He suggested the two groups could ultimately work on ways to mesh activities on various audio and video security schemes to ensure there is a single, efficient copyright protection system — not two parallel ones, one for video and one for audio.

Bell noted that while video and audio could share the same encryption technology, they would require different watermarking schemes. For instance, in video, watermarking uses psychovisual effects, while audio relies on psycho-acoustic effects.

"Not until it's clear how all the technologies interlock can the implementers have confidence to move forward with their plans or the content providers have confidence to make their content available," Bell said.

Recording groups have done some work of their own on audio security. The International Federation of the Phonographic Industry created a project called MUSE, whose goal was to find a way to embed identifying information within its recordings for security purposes. The MUSE project partners include RIAA, Telstar and the international arms of BMG, EMI, Polygram, Sony, Universal and Warner.

Based on such work, Scott Moskowitz, chief executive officer of Blue Spike Inc. (Miami) and the inventor of the company's Giovanni digital watermarking technology, said he is optimistic SDMI could meet its goals. "They've done a fair amount of testing," he said. "They already understand that security is a software issue, not an issue of a box or processing power of a CPU."

A number of semiconductor companies have also expressed general support for the SDMI effort. Michael Moradzadah, director of strategic planning for home products at Intel Corp. (Santa Clara, Calif.), said Intel has worked closely with the CPTWG and is evaluating SDMI's mission.

Gary Johnson, manager of the digital audio program in Texas Instruments' emerging-markets group in Houston, said TI got involved because it wants to

make sure there's enough music available online to create demand for the digital music players for which it plans to supply DSPs.

"We don't back any standard [for digital music] or encryption format," said Johnson. "Our chips are programmable and will work with any of the standards out there. But until the big five labels put their music online, there won't be enough demand for a digital music player with a TI DSP."

Another backer, Lucent Technologies (Murray Hill, N.J.), has worked with the music industry on security initiatives and its PAC codec. PAC was used as part of a New York-Los Angeles live Internet demonstration last October, where the music industry showcased high-quality audio over the Web and watermarking technology from Cognicity Inc. (Minneapolis).

— Junko Yoshida contributed to this report

Government Affairs

Site Navigation

- [ITAA Home Page](#)
- [Government Affairs](#)
- [Legislative Activities](#)
- [Net Issues](#)
- [State Legis-Link](#)
- [HR Issues](#)
- [Year 2000 Issues](#)
- [Congressional Hearings](#)
- [Publications](#)
- [Public Policy Report](#)
- [ITAA Publications](#)

Search the website:

Submit Query



Information Technology
Association of America
1616 N. Ft. Myer Drive
Suite 1300
Arlington, VA 22209
(703) 522-5055
(703) 525-2279 (fax)

Western Region Office
One Market Street
Suite 2700
San Francisco, CA 94105
(415) 267-4055
(415) 267-4198 (fax)

Problems or questions
about the site? Contact
our [webmaster](#).

ITAA Publications

Intellectual Property Protection in Cyberspace: Towards a New Consensus

Executive Summary

When it comes to the Internet and government policy, the indecency issue has garnered the greatest attention over the past year. However, over the long term, intellectual property protection will in all likelihood prove to be the more important concern because of the need to make the Internet economically viable. At the heart of the matter is a paradox: How to protect ownership of copyrighted material while at the same time making digital works widely available over the Internet and other online services.

Industry self-regulation and innovative new technology may hold the answers. In the field of intellectual property protection, cross-industry cooperation and self-regulation can enhance digital copyright protection and spread the value of Internet and the World Wide Web to a wider audience, serving to increase, not devalue, the worth of the copyright.

While technology is blurring traditional lines of copyright protection, particularly in the once discreet areas of distribution, reproduction, and transmission, there remains a basic premise – regardless of whether the work is in analog or digital form – that unauthorized reproductions are illegal. There is no question that if content distributed over the Internet is infringed, copyright holders will simply refuse to make valuable works available on the Internet and related online services. Similarly, requiring Internet access providers to place cumbersome or confusing controls on that same content, or requiring them to monitor or police content, will be inefficient and ineffective, alienating consumers and lessening the likelihood that cyberspace will realize its full potential.

Copyright protection measures which result in singling out Internet access providers, and legislative proposals which attach liability unfairly to access providers, will undoubtedly undermine the delivery infrastructure, forcing these companies from the marketplace and making access to the Internet more difficult.

Copyright holders, content providers and Internet access providers have a mutually dependent relationship – quality online content increases demand for Internet access, while increased Internet access increases the demand for quality online content. Absent significant cooperation among content and access providers, the Internet can easily dissolve into a muddle of competing and parochial interests.

This paper explores the current environment surrounding digital copyright protection and attempts to spark a new and necessary dialogue between the interested parties. In order to resolve the paradox, all parties in the debate must cooperate.

ITAA believes that the economic stakeholders in this discussion include:

- Copyright holders who are seeking assurance that their content is reproduced and distributed only when authorized. They seek to identify infringers, and to get unauthorized reproductions removed

- expeditiously.
- Internet access and service providers who seek to establish "on-ramp," network connection functions without excessive and unreasonable exposure to copyright infringement liability. They seek to deliver content to their customers without being required to monitor the billions of bits of information (unidentifiable and never transmitted in one piece) being transmitted every day.
 - Online providers who operate bulletin boards, chat rooms, home pages and related facilities which may – absent legitimate copyright holder notification – have an unauthorized reproduction of a digital work posted by a user without knowledge of the provider.
 - Internet software companies who provide applications like Internet navigation and browsing products, and have no control over or knowledge of transmissions which may violate copyright.
 - Common carriers who simply transmit packets of content from a content provider (whether authorized or unauthorized) to an end user.

These groups are the immediate community of interest when considering digital copyright protection. Additional interested parties in the outcome will include lawmakers, government officials, the media, "fair use" entities such as libraries and universities, and, of course, end users.

ITAA believes that a "delicate balance" involving a combination of legislation, education and technology is required to satisfy this varied collection of stakeholder interests. To date, too much attention has focused on government's role in attempting to "settle" the dispute, on both the federal and global levels. While there is a legitimate and potentially useful role for the government to play, the ultimate success of the Internet rests on agreement within the digital community.

At a minimum, this agreement must incorporate three principles:

1. Clarification and enforcement of current copyright law.
2. Education of end users to reduce dramatically inadvertent copyright infringement.
3. Utilization of copyright protection technologies. The marketplace already offers a variety of technology-based solutions, responding to a variety of copyright protection requirements. The richness and diversity of these offerings will only increase in the near future.

Section One of this discussion paper elaborates on these principles. The discussion centers on a series of important questions, including:

- Why do current legislative proposals - both nationally and internationally - fail to balance stakeholder interests?
- How can cooperation among the interested parties be achieved?
- What is the desired "end state" for copyright protection on the Internet, and how can the "delicate balance" of interest groups be achieved?
- What human behaviors can be stopped, and what individual freedoms must be preserved?
- What role can an effective consumer education program play?
- Assuming that technology solutions do provide protections sought by content providers and do gain wider currency, what adjustments to current law are necessary?
- If technology is the answer, what functions must this copyright protection technology perform?

Too often, discussion surrounding digital copyright protection fails to take

into account the physical and practical limitations imposed by the Internet itself. Section Two outlines the "architecture of the Internet" and the technological difficulties presented by various proposals to reduce the transmission of infringing works, such as: monitoring, taking down, identifying without knowledge, and other such proposals. The IT industry is concerned that attempts to legislate sanctions to digital copyright protection and infringement may ignore technical realities.

The physical operation and working dynamics of this "network of networks" defy traditional legal notions of enforcement, boundaries, and liability. This portion of the paper attempts to put the situation in perspective.

For instance, the interested parties in this debate need to ask:

- Is "take down" - even if given "compliant notification" - always economically and/or technologically feasible?
- What if the access provider has no ability to effectively "take down" the unauthorized transmission?
- Which, if any, access providing parties along the chain of distribution have any reason to know (absent notification) what is contained in the package being sent? What is the content? Who is authorized to send or receive it? And does an access provider have any ability to control its transmission?
- If there are a series of "acceptable" reproductions of digitized transmissions, e.g. through routers and browsers, and into cache and random access memory, how is an access provider to know when a particular transmission is not authorized?
- How much "control" is lost because of the transparent nature of the Global Information Infrastructure, and the fact that national boundaries are non-existent?

While not offering definitive answers to each of these questions, this section cuts through simplistic solutions and advances a more realistic discussion by introducing an important, and oftentimes missing, technical context.

Just as people can use technology to infringe copyrights, people can use technology to stop it. Section Three documents the abundance of technology-based copyright protection choices. This extensive (but not exhaustive) compendium identifies and categorizes specific products, explains how each is used, and provides related company contact information. While this varied range of products strongly suggests that the marketplace is responding to the digital copyright protection needs of copyright holders, users and others, this initial collection is only a starting point. ITAA will continue to identify products, maintain this list and provide it to all interest parties.

Industry-led, technology-based solutions can be helpful in reducing the transmission of infringing works and restoring a sense of balance and clarity to an otherwise difficult situation. Through a discussion of principles, an exploration of what is technologically feasible, and a review of products and promising technologies that can protect copyright, ITAA seeks to move the state of thinking forward. Stakeholders should place the focus of discussion where it properly belongs and where corrective steps will be most effective: on industry self-regulation and copyright owner self-protection.

Section One

The Current State of Affairs Regarding Digital Transmissions in Copyright Law

A. Legislation/Government Action

Legislation originally introduced in the 104th Congress failed to protect the legitimate interests of all stakeholders in the copyright protection debate. Two bills in particular – H.R. 2441 and S. 1284 – sought to amend U.S. copyright law and adapt it to the digital age, reflected recommendations of the Administration's Information Infrastructure Task Force Working Group on Intellectual Property Rights. Introduced by Representative Carlos Moorhead (R-CA), then-Chairman of the House Intellectual Property Subcommittee, and Senator Orrin Hatch (R-UT), Chairman of the Senate Judiciary Committee, the bills were intensely debated at a number of hearings and were the subject of stakeholder "negotiations" through the spring of 1996.

The World Intellectual Property Organization (WIPO) has also been attempting to assert preeminence in digital copyright protection internationally. A Diplomatic Conference has been scheduled in Geneva in December of 1996 to tackle the digital copyright issue.

The IT industry in general and the membership of ITAA in particular fully support the need to protect the rights of copyright owners and the need to balance their rights and obligations with those of information publishers, distributors and users. Legislation introduced in the last Congress and WIPO's draft international treaty language, however, fail to address the single most problematic issue facing the online services industry: the assignment of direct, contributory and/or vicarious copyright liability to online services providers for their alleged "role" in the transmission of infringing material on their networks. On the contrary, the federal legislation and WIPO treaties, as proposed, extend to copyright holders and content providers a new "transmission right" over their works – a move which appears sure to attribute liability to companies innocently or unknowingly involved in the distribution of unauthorized reproductions.

An impasse over the Congressional bills seemed to be resolved when online service and Internet access providers agreed to support an "upon notification" approach which would have them quickly remove infringing works from servers within their control, when formally notified by the copyright holder or their agent. Creating such an expectation of responsible action on the part of access providers would be no more or less stringent than that placed on booksellers, music dealers and others trading in copyrighted works. Progress towards markup evaporated, however, when the electronics industry took issue with portions of the bills related to "time shifting," the functionality of computers and home electronics equipment which allows users to record digital works for subsequent playback. Congressional work on a digital copyright bill has now been postponed until 1997. The legislative activity left in its wake, however, hints at the cooperation which is possible among the stakeholders.

B. Enforcement of Current Copyright Law

Regardless of future amendments and/or clarifications, copyright holders should be able to depend on rigorous enforcement of current copyright law. In the non-digital realm, current law protects the rights of content providers while preserving the delicate balance among all the interested parties. Existing law can also work well in cyberspace—if it is clarified in some instances and enforced in others.

Currently, all content available in cyberspace is protected under copyright law. The inadequacies in the copyright law are not unique to the online world; instead, they illustrate how copyright law must evolve, both in the digital and analog worlds. Even in the digital world, once the infringement is discovered and the infringer identified, current law is generally sufficient for prosecution.

Because the Internet is relatively young, the volume of case law on this issue is relatively small. Nevertheless, a few cases have explicitly held that copyright protections extend to works in cyberspace. In 1993 a federal district court in Florida held that distribution of copyrighted photographs by an on-line operator violated the copyright holder's rights of distribution and public display. A federal district court in California held in 1994 that the on-line distribution of copyrighted software constituted a direct infringement of the copyright holder's rights. These two cases are classic examples that current copyright law does, in fact, apply to cyberspace.

Moreover, Internet access providers have shown their willingness to help enforce current copyright protections. Recognizing that digital copies are nearly perfect and can be distributed nearly instantaneously, access providers have expressed a willingness to "take down" infringing material where there is a "compliant notification" and the technical ability to do so, even without a court order, so long as they are not held liable for the infringement and are covered under a "safe harbor" provision if the "take down" was deemed to be ultimately wrong.

Even if technically possible, this proposal may not be as easy to implement as it appears. Privacy issues, particularly with respect to e-mail communications, remain a major concern. In the United States it is illegal to monitor electronic communications under the Electronic Communications Privacy Act (ECPA). Under international privacy norms the issue is even more restrictive. Any new laws dealing with the monitoring of electronic communications will have to survive these firewall protections, as well.

There are, however, specific areas whereby current copyright law must be refined to work better in a digital world. And again, in making these enhancements, questions of balance and common sense come into play:

- The ability to quickly and widely distribute digitized content requires new procedures for "taking down" unauthorized transmissions. Copyright holders would like to have the ability to notify access providers and within a reasonable amount of time—and without going to court—have the content removed.
- Access providers, who have no knowledge of and/or control over an infringement, should not be held liable (directly, vicariously or contributorily) for such infringements.
- Knowing copyright infringers should be prosecuted, regardless of whether or not they profit from their infringing activity. Copyright infringement devalues intellectual property; such losses occur whether or not the infringer gains monetary rewards.

Case law illustrates the need to adjust copyright law in this new digitized information age. In *United States v. LaMacchia*, a Massachusetts court in 1994 held that an MIT student who made hundreds of copyrighted computer programs available without charge could not be prosecuted because he did not economically profit from his actions – he simply

devalued the copyright owner's property. Loopholes such as this one must be closed to ensure that when the value of a copyright is destroyed or severely devalued by a malicious infringement – whether or not an economic benefit is received - the full force of copyright protection must be applied.

Senator Patrick Leahy (D-VT) tried to close this loophole in the last Congress. His bill, S1122, would have removed the "for-profit" requirement for copyright infringement. Under the Leahy proposal, the initiator of the infringement could be prosecuted, not only when copies are made for personal financial gain, but also when there is a resultant devaluing of the copyright, regardless of whether or not the infringer personally profits from the unauthorized reproduction or distribution. The legislation, unfortunately, languished in the Senate Judiciary Committee, however, ITAA will be working with the Senator to have the bill enacted in 1997.

Clarity and fine-tuning are also necessary in areas where courts have not yet explicitly ruled. One such area was explored in *RTC v. Netcom On-Line Communications Service, Inc.*, dealing with the liability of an Internet access provider for use of its service to access and distribute copyrighted material. In this case, a named defendant placed copyrighted works of the Church of Scientology on a bulletin board linked to the Internet via Netcom, an Internet access provider. RTC, the copyright holder of the works in question, brought suit to enjoin the defendant from distributing the works. The court held that access provider liability should be judged on the basis of a contributory infringement claim. Because the access provider did not have "actual knowledge" of the infringement and did not receive direct profit from the infringement, it could not be held directly liable for the violation. This decision, however, did not settle the question of the actual level of liability of an access provider. It has thus been left to either the courts or Congress to address this issue.

Finally, the issue of permitting access providers to make necessary transmission reproductions to bring the digitized content to end users, and then allowing individuals to download and view the content, is also contentious. Some argue that content providers already grant an explicit, or, at least, implied license to "reproduce" and "transmit" when they initially place their work on the Internet. Those who distribute digitized work online know at the outset that it will be "reproduced" (and not completely intact) from computer to computer, router to router, browser to browser, transmitter to transmitter, as it is being transmitted from site to site to reach the end user. Additionally, the practice of caching, or storing a copy of a given work in a faster location to improve overall Internet performance (where the access provider and/or the end user has the content stored in a cache in computers' random access memory (RAM)), is prevalent on the Internet. The copyright holder, the courts and Congress must come to grips with the validity of such implied licenses if the Internet is to be used as a major means of content distribution.

Some have argued that the statutory defense of "fair use" – which allows a party to use portions of copyrighted material for certain purposes without having to seek permission from the copyright holder – may be applicable to access providers and end users. This approach seems to be unworkable for a number of reasons, including the fact that the concept of "fair use" is not recognized globally as a reproduction defense.

- Can current copyright laws be enforced sufficiently to protect online content – and to what extent?

- · Do the currently proposed legislative and/or international treaty solutions close the loopholes sufficiently or present new problems?
- · Does a copyright holder grant an implied or explicit license to reproduce at the various and necessary transmission points of distribution when content is digitized and placed online?
- · Will the "notice and takedown" concept work within the realities of what is technically feasible and economically reasonable?
- · Should not copyright enforcement focus on the "initiator" of the infringement (unauthorized reproduction) instead of placing liability on the "facilitator" of the transmission (Internet access provider)?
- · Does a hyperlink violate a copyright if it serves only the purpose of pointing to a site, and that no other connection (economic benefit from or actual knowledge of) to that site exists?

Interested parties must work together to address these questions, to reach consensus on difficult issues like these and to enhance current copyright law in ways which maintain the "delicate balance," providing the fullest possible protection of digital works while safeguarding the future growth of the Internet and other online services.

C. Education of the End-Users

The NII White Paper properly recognized that education "of the importance of intellectual property in the information age is essential." Education is a key facet of the discussion; first, because there is a distinction between the individual making a private copy for personal use and the pirate making wholesale counterfeit copies for financial gain or to destroy the value of the intellectual property. Although no level of copyright infringement is acceptable, infringement which causes little if any economic deprivation to the copyright holder already occurs in the non-digital world and has been tolerated by content providers. Public education and awareness can, however, significantly decrease the extent to which such infringements take place in cyberspace, and could serve to lessen even "innocent" infringements.

Educational strategies, however, must work in combination with technology controls to make the controls themselves comprehensible and acceptable. Infringement "alerts" could include warning screens, advertisements and penalty notices by the access providers. One such initiative is Project OPEN, sponsored by the leading online and IAP companies, by the National Consumers League, and by the Interactive Services Association. Project OPEN is working to educate consumers through its "Bytes Have Rights" campaign, which delivers important messages to end-users about the implications of online copyright violations. Consumers are advised to follow the rule – "If in doubt, don't use or copy it."

Additionally, the Working Group on Intellectual Property Rights has initiated the "Copyright Awareness Campaign" in conjunction with the release of the NII White Paper. This effort brings together educator associations, media organizations, copyright owners, the Copyright Office, and the Departments of Education and Commerce to determine the best way to educate the public on the importance of copyright protection.

The Business Software Alliance has instituted an "Anti-Piracy Program" which takes a three-pronged approach to copyright protection: education, policy, and enforcement. BSA feels that the general public must be strongly educated and persuaded to not make copies of digital content without authorization.

By engaging in an industry-wide voluntary program that educates

end-users, the information technology industry plays an important role in communicating to malefactors that copyright infringement is a crime, that the offender will be prosecuted, and that the penalty can be substantial.

D. Technology Tools

Even if legislation were passed that makes necessary adjustments to current copyright law, and consumers were adequately educated, many in the information technology industry believe additional marketplace solutions are still essential to ensure the long term success of the Internet. The NII White Paper recognized the role technology will play, stating that "content providers will rely on a variety of technologies, based in software and hardware, to protect them against unauthorized uses of their information products and services." When copyright holders and content providers begin to utilize the many and varied technological tools that can serve to protect video, audio, and text-based intellectual property distributed in a digitized form over the Internet – choosing the level of protection based on the value of the content and limits they wish to place on reproduction – most of the problems expressed during the Spring 1996 Congressional debates will be silenced.

There are already some technology tools today, and many more in development, that can securely label intellectual property and provide the means for those who have control and have been given notification of the infringement to monitor, take down, and/or block infringing material. The NII White Paper stated, "Technology can provide solutions for these needs. Technological solutions exist today and improved means are being developed to better protect digital works through varying combinations of hardware and software."

Copyright owners and content providers have the tools available to label, tag, or add a digital watermark to the work at the beginning of a transmission's "food chain," before it is sent out onto the Internet. Depending on the perceived value or importance of the work, the copyright holder can "wrap" the package with various levels of protection. These protections can restrict reproduction, use, re-transmission, and provide the means necessary to identify, locate, impede or take down unauthorized reproductions. This technology approach maintains the value of copyrighted material.

Leveraging such tools, and working closely with access providers and end users, copyright holders will be empowered to make protection and enforcement decisions for themselves, instead of being shoe-horned into a one-size-fits-all legislative "solution." For example, copyright holders and content providers who desire the utmost security can choose encryption technologies that allow for secure transmission to only those with whom the owner has a direct relationship. A copyright holder can even limit the use of content to a single authorized "customer." Digital watermark technology places special codes in audio recordings and visual arts to help identify the purchaser and prevent infringement without destroying the work itself. Technology also offers an approach which involves labeling infringing web sites and blocking access to them.

The same technology that enables the lawful and authorized distribution of digital content promises the potential to identify and track unauthorized reproduction, as well. When crafting the application of the technology, all of the stakeholders must, however, be sensitive to the privacy issues on both a national and global scale. The latest versions of both Microsoft and Netscape web browsers, for example, have the ability to track the identity and usage of those who access each web page. Additionally, companies

such as CyberCash offer the potential to facilitate payment of royalties for online usage while at the same time tracking the identity of the purchaser. Future copyright protection tools will only become more precise, sophisticated, enabling and empowering. The Platform for Internet Content Selection ("PICS") which was initially developed, for example, to empower families with the ability to control access to indecent content, can be adapted in the copyright protection arena, as well.

These technologies could severely limit an infringer's anonymity, enabling access providers, as soon as they are given compliant notification, to track and take down unauthorized reproductions. By assisting content owners in learning the identity and possible location of the infringer, proper steps can then be taken to enforce copyright laws already in place.

Moving forward, the discussion will shift to address questions like:

- If the relative cost of efficiently "tagging" valuable content before it is distributed is minimal and widely available, under what circumstances should an access provider be held liable if the content provider or other responsible party fails to notify the access provider of an alleged infringement?
- Are there technological limitations with respect to the ability of an Internet access provider to be able to take down and/or block infringements, even if there is a notification?

Summary

The ultimate success of the Internet requires copyright owners, content providers, Internet access providers, and digital content users to cooperate in finding ways to limit unauthorized reproductions and to impede, prevent and identify infringements. If there is a common-sense balance to the enforcement of copyright law, an effective educational campaign of end users, and significant use of copy protection technologies, the Internet will become bigger, fuller, richer — an information utility analogous to universal telephone service or the electrical power transmission infrastructure. What factors must be in place, however, to encourage and preserve cooperation among all parties and, as a result, to achieve this vision of the Internet? In short, on what issues must consensus be achieved?

For the Internet to succeed, digital copyright protection must be:

- **Empowering.** Content owners must have the ability to and must take primary responsibility for securing, identifying and tracking distribution of their copyrighted works – and maintain the rights they have been given in copyright law. Copyright holders must be able to define the level of protection they desire and need to maintain the value of their intellectual property.
- **Convenient.** Copyright protection must be implemented in ways which do not unreasonably encumber content users or raise inappropriate access barriers. If access providers are required to police sites and/or monitor transmissions, the Internet will become useless.
- **Fast.** Tools and techniques to protect copyright cannot significantly reduce system response times or otherwise detract from Internet performance.
- **Secure.** Copyright protections must feature a high degree of security, thereby delivering the desired access controls and defeating unauthorized attempts to gain access to copyrighted works.

- Robust. All parties benefit when rich content is available on the Internet. Copyright protections must facilitate the availability of such content, providing new means for content owners and service providers to offer protected material to the public.
- Fair and Reasonable. Copyright protection on the Internet cannot favor one group over another but must apply equally to all segments of the marketplace.
- Enriching. Innovations such as the printing press, photocopier, personal computer, facsimile machine, video cassette recorder, and other tools of communication have demonstrated that technology can, if properly channeled, greatly amplify the value of copyright to the copyright holder. Protecting content in the Internet environment must be consistent and have this same effect, leveraging the power of the network for buyer and seller while controlling the distribution of protected works.
- Accessible. Protections must not become economic, cultural, social or political barriers to access. Rather, effective digital copyright protections will reinforce the Internet's potential to become the global information utility.
- Affordable. Both the technology tools that protect content and the technology which delivers that content must remain affordable.

Section Two

How The Internet Works

Introduction

How well does copyright enforcement translate to the digital environment? This section examines the practical realities of this issue by looking at the physical and logical dimensions of the Internet. Too often, copyright discussions treat the technology as an abstract—with no consideration given to the feasibility of creating the desired copyright controls. The "negotiations" held during the Spring of 1996 between the content and Internet access providers under the auspices of Congressman Bob Goodlatte (R-VA) would, no doubt, have been more productive had they been grounded in a better understanding of the underlying technical issues involved. It is important to recognize that the actual functionalities of the Internet, just like the laws of gravity, cannot be legislated.

Significant limitations do exist. Content is converted into data; the data is broken into unrecognizable digital packets; and the packets are subsequently disassembled and reassembled. Transmission of a single file involves multiple organizations, multiple devices facilitating transmission, and multiple jurisdictions. The nature of the technology itself makes content control, monitoring or protection at points along the network problematic, if not impossible. By the same token, encryption or encoded technology, appropriately applied before and after transmission, can effectively protect content and preserve copyright.

To understand why technology is both an obstacle and an answer to digital copyright protection, it's necessary to take a closer look at the inner workings of the Internet.

The Internet and How it Works

The Internet is a global "network of networks." In physical terms, the Internet is a vast international collection of networks, computers and software, all working together to form the world's first digital information

infrastructure. Originally envisioned to interconnect no more than 256 networks, today the Internet links tens of thousands worldwide.

The Internet is interconnected in a series of local nodes and regional hubs. Users gain access through commercial online services such as America Online, Prodigy or CompuServe; through Internet service and access providers (ISPs and IAPs) like MSN, Netscape, MCI or AT&T WorldNetSM Services; or through a private network gateway, such as that which might be maintained by a corporation, university or government agency.

No particular company, group or national government owns the Internet. In a sense, the Internet is a phenomenon which has no beginning and no end, but rather a series of networks constantly added and removed as participants come and go. Should failure occur in part(s) of the system, the rest of the Internet continues to function. No single organization holds responsibility for its proper operation. Indeed, no one owns the Internet; rather, it is a "shared resource." The extent to which the Internet continues to serve as the world's information infrastructure will be a direct result of its voluntary, democratic and unregulated nature.

Common standards have provided the compatibility required by the otherwise disparate technical components of the Internet. For instance, a standard networking protocol called TCP/IP provides interconnectivity among the thousands of smaller networks. Similarly, compliance with a standard application programming interface like sockets allows programs to share text and data across the network. A common language, Hypertext Markup Language (HTML), provides a standard text file format.

The Internet is divided into a series of levels. The World-Wide Web is the layer of the Internet which provides multimedia content, organized in a series of graphical home pages. WWW content is located and accessed with tools called web browsers. In the early 1990's, developers at the National Center for Supercomputing Applications (NCSA) created the first well-known tool for browsing content on the Internet: the NCSA Mosaic program. Although browsers today might contain many user interface distinctions and other features for market differentiation, all capitalize on the basic principles demonstrated by NCSA. Operating and looking the same on UNIX, PC, and Macintosh computers, NCSA Mosaic fundamentally changed the way that people used Internet tools, making the experience relatively uniform.

As noted, browsers have added new features and benefits, and will continue to do so, enabling the user to experience the benefits of sound, video, 3-D graphics and more. In a sense, today's browser is somewhat analogous to a Dolbyä sound system, which takes a signal which might otherwise be unusable or unpleasant and, through special packaging or an enhancement, adds substantial value to the original, sometimes simply making it perceptible to the end-user.

Browsers display the information located at web sites. Browsers work in conjunction with various directory publishers and their search engines: These engines index web site content using the standard labels attached to Web documents, termed Universal Resource Locators (URLs). Retrieval is accomplished in different ways and with varying degrees of sophistication and precision.

The momentum of the WWW has tended to overshadow other aspects of the Internet. The Internet offers a variety of text-based services: e-mail, newsgroups, and file downloads. Just as browsers are used to navigate on the WWW, a variety of tools allow users to mine this text-based substrata

of the Internet, which include e-mail, newsgroup readers, FTP clients, Gopher clients, wide area information server (WAIS) clients and more.

Briefly, these tools perform the following tasks:

- E-mail tools allow messages to be created, managed and exchanged over the Internet
- Gopher clients navigate the menu-driven structure of Gopher servers to locate precise information
- Newsgroup readers deliver newsgroup content with features which facilitate screening and prioritization
- WAIS tools search database content for key search terms—as opposed to just scanning heading labels
- Other text-based tools include Archie, Veronica and Jughead. Archie is used for file transfer from FTP sites; Veronica provides exhaustive Gopher site searching; Jughead offers specified Gopher site searching.

Even these distinctions between tools are rapidly becoming arbitrary, called into question by the ability of many Web browsers to either provide these services or to be packaged and integrated with tools which do.

The Internet, unlike the text-based networks of the past, features a wide variety of data types. While much of its content remains text, many content providers on the WWW are now using rich data in the form of still images and audio. Moreover, compression routines, advances in CPU power, new standards and other innovations are making the introduction of video, three-dimensional data, real-time audio and animation commonplace.

The Building Blocks: Hardware, Software and Data

The Connection

Each computer must be connected to the Internet through some sort of service. Users generally connect to the Internet through an access or service provider, sometimes by way of a dedicated leased circuit, but usually via dialed connections established when needed. Typical consumer usage involves dialed connections, and the description which follows focuses on dial-up users (except where noted).

At a technical level, IAP facilities consist of modem, terminal servers, and other equipment enabling users to establish a session; Internet Protocol (IP) routers, leased circuits, and other connectivity infrastructure; various servers operated directly by the IAP for email, news and other content; and, routers and leased circuits, providing connectivity to the Internet at large.

Modems convert digital signals into analog signals so that they can pass over normal telephone circuits. At the other end, the opposite process takes place: the analog signal is converted back to a digital data stream. An IAP will typically have many modems available and configured so that users dialing a single telephone number will be randomly connected to any one of the modems. Once the user is connected to a particular modem and the session is established, all data passing between the user and the IAP in either direction will pass through that modem. A modem concerns itself only with the correctness of data bits and makes no interpretation of the content of the data being passed.

The analog side of a modem is connected to a telephone line. The digital side of a modem is usually connected to a serial port on a terminal server.

A typical terminal server will have up to a few dozen modems connected to it. The terminal server converts the data received from the modem into the format required for the rest of the IAP infrastructure. Only the network-specific portion of the data is changed; no access to the content of the data is performed. The terminal server controls the physical activity of the modem, acting as an "onramp" or Internet access point, for the IAP, collecting and submitting authentication information (ID and password) to a server elsewhere in the IAP complex.

When data leaves the terminal server via the local network ("LAN") connection, data from the active modems are interleaved as needed in the data stream and sent to the LAN. Usually, the LAN itself is fairly small and is used merely as a high-speed conduit to an IP router. The IP router shuttles packets from one of its input ports to one of its output ports. The ports can be the entry way to LANs, high speed dedicated circuits, or other networks facilities. Routers are "stateless," which means they route each block of data individually and do not remember how they routed previous blocks. Routing decisions are made based on header information (never on content data) and controlled by a combination of configuration information and dynamic routing protocol information.

Packet Switching and Caching

The routing decisions are facilitated by packet switching. Packet switching is a technique used in data networking to lower the cost of dedicated circuits and to avoid congestion at various network nodes. This technique involves breaking data into packets, each with its own individual address. An apt analogy is to think of a group of co-workers traveling to a meeting. All leave a common address – the office – for a common destination – the meeting. Each worker, however, can take any number of routes throughout the city to reach their destination. At any one point in time during travel, it would be nearly impossible for the boss to know the location of all the travelers.

The packet also contains the information necessary to properly sequence data once it arrives at the address site. The packets can be analogized to traditional mail. The packet headers act as envelopes, providing all relevant addressing information. At the same time, the payload (content) remains shielded from the details of delivery. IAPs will usually offer two or more physically diverse paths between any two points to promote reliability. In the event of the failure of a single telecommunications link, the other links can continue to carry the packets. A router can tell when a link has failed or is degraded. In such a case, or when otherwise configured to do so, a router will favor one link over another when routing packets. In general, however, physically diverse paths that connect to the same distant point will be considered equivalent. Packets have an equal chance of being routed over any of the equivalent links. In fact, two consecutive packets from the same source to the same destination will often be routed over different links. Since there are many routers and many links between typical sources and destinations, the packets from a data stream can individually travel widely different paths.

Internet providers use a variety of techniques to improve the speed and reliability of data delivery to the end user. Packet switching, as described above, is such a technique, having the possibility to improved both the speed and reliability of data delivery. Caching is another tool employed by Internet providers to improve network performance. Caching involves storing often-accessed data on special high-speed servers or on local machines for quick access. By reducing the travel distance on the Internet (and thus, network traffic) on the Internet, caching greatly improves access

speed and the speed of data delivery to the end user.

Additional Services

Most IAPs offer services beyond mere IP routing. These services might involve electronic mail servers, usenet news servers, "chat" conference servers, DNS (domain name system) servers, web servers, file storage areas on FTP (file transfer protocol) servers, or HTTP (hypertext transfer protocol) proxy servers. These services will be operated on one or more general purpose computers within the IAP's complex.

At some point, links from routers connect not to other parts of an IAP's infrastructure but to routers belonging to other IAPs or third parties. There is little technical difference between the movement of packets within the facilities operated by the IAP and the movement of packets into, across, and out of the Internet.

Putting the Pieces Together: The Practical Realities of Copyright Protection

Due to the architecture and technologies of the Internet, only two truly effective points of control and enforcement exist: the point of transmission and the point of reception. Packet switching, caching, and routing make any other control nearly impossible.

Cases involving inadvertent copyright infringement could be handled through a formal notification process by the copyright holder or the content provider to the IAP, after which the site operators would, if technically feasible and economically reasonable, remove the infringing material from the site.

But suppose there is a place on the Internet, "scofflaw.example.com", which habitually hosts material in violation of international copyright agreements. Is it technically possible and economically feasible for an IAP to block access to the site, preventing customers from obtaining material from that site via communications links that the IAP controls?

The answer is that this cannot be done in any practical, economically feasible way, for sites not hosted in the IAP's servers. Before getting into the details of why it's not possible, it's worthwhile to explore some underlying principles.

There are many competing products on the market today which will allow users to voluntarily limit the content that they wish to be able to access. Generally, these are software "filters" which are marketed under the category of parental control. The intent is that parents and community leaders can use these products to prevent children from viewing content that they consider to be violent, pornographic, or otherwise unacceptable. Accompanying the software filters are databases of site content ratings prepared by some third party. It would not be a difficult matter to add copyright-infringing sites to the database. At best this kind of technology only covers voluntary participation by responsible IAP customers who will, figuratively and literally, ignore the infringing site. It is important to note, however, that screening technologies are only effective after the infringing material has been made available.

Even if attempts at access could be effectively screened, site operators would make the material available via more circuitous access methods. IAP customers, knowingly or otherwise, will use the more circuitous access methods. A site name is more the name of a logical place than a physical

place. A given site name may actually span several machines; on the other hand a single machine may actually host several different logical site names. The consequence is that blocking access to a specific site is actually an imprecise undertaking. One may actually be blocking access to several sites, only some of which are infringing copyright.

The contest between site operators trying to provide access to infringing content and the IAP trying to prevent access can be characterized as an escalating strategy and counter-strategy situation. The IAP implements techniques for preventing one method of access, and the infringing site's operator will invent new access techniques. Meanwhile, the effort on the part of the infringer is relatively small in the overall scheme of Internet access. Correspondingly, the job of the IAP in separating attempted access to legitimate materials from access to infringing materials is extremely complex and resource intensive.

Infringement and Enforcement: Three Examples

A user comes across this URL:

<http://www.scofflaw.example.com/some/path> This is a web site containing infringing material. The user decides to check it out.

Approach 1: Host Name Blocking

Behind the scenes, web browsing software translates the host name ("www.scofflaw.example.com") into an IP address (e.g., 192.1.1.34), a process known as host name resolution. The IAP could configure the local Domain Name System (DNS) not to translate the names of infringing sites. When the customer software attempts the resolution, the IAP DNS server would respond "no such host", "server error", "administratively prohibited", or some variant.

This approach is easily defeated in a number of ways. Although an IAP typically instructs the customer to configure the software to point to one or more IAP-controlled DNS servers, there is nothing preventing the customer from specifying other DNS servers. Such servers could be anywhere in the world, perhaps even under the control of the infringing site. Since the algorithms under which DNS operate generally assume that every visible DNS server can find the answer to any given DNS query, detouring to a different DNS server is no problem.

An IAP could prevent this user's DNS queries from leaving the IAP-controlled facilities, in effect forcing the customer to use the IAP-controlled DNS servers. This approach is undesirable for at least two reasons: first, it places providers at a competitive disadvantage because not all IAPs will impose this restriction. Second, such a move is hazardous to the IAP's own DNS operation, adding a significant new level of complexity.

And even if an IAP forces all DNS queries to be done via IAP-controlled DNS servers and then blocks resolution of infringing site names, the user still reaches the site by directly specifying the IP address rather than host name in the URL:

<http://192.1.1.34/some/path>

as opposed to

<http://www.scofflaw.example.com/some/path>.

In this manner, the user easily sidesteps controls placed on the translation of host names.

Approach 2: Packet Filtering

Individual filtering of packets based on their content would be impossible. Because data is broken into non-continuous blocks, it is not possible to determine the content of any packet while it is in transmission. Only once the packets have been reassembled on the end-users computer can they be understood for their content. As a result, packets must be filtered according to their origin, not their content.

The IAP may attempt to block access to infringing sites through adjustments to IP routers. Packets move on the Internet according to IP addresses. IP routers direct this traffic. The filtering rules for these devices could be programmed to selectively reject packets based on various criteria like source or destination IP address. There are, however, significant problems with this approach.

A given server can have a large number of IP addresses assigned to it; all of which are easy to change. The IAP would have to constantly consult DNS for changes in the IP address list for an infringing site, and then revise and re-install the filtering rules on the routers to account for any changes.

A far larger problem, however, is the sheer number of filtering rules which would have to be in place. Imagine hundreds or thousands of infringing sites being listed for blocking at any given time, and imagine several possible IP addresses for many of them. Even if the attempt were made, router performance would be degraded significantly, becoming much slower at routing packets through the network. Unable to keep up, routers would begin to discard other packets (which have nothing to do with infringing sites). Even a relatively small number of lost packets can begin to cause serious problems in a network. As packets are lost, the originating hosts resend them, consuming more bandwidth and router processing.

The added filtering requirements not only degrade performance, they diminish security. An IAP uses router filters to protect its customers and its own infrastructure from accidental or intentional intrusions. The added complexity of the filtering rules (and the large number of new rules they represent) creates a threat to the IAP's security plans. Given that the rules would have to change quite frequently, the chances of accidentally misconfiguring the router is increased enormously.

Approach 3: Blocking HTTP Proxy Servers

Even if an IAP accepted the administrative, security, and performance costs of packet filtering for some number of infringing sites, access control would be ineffective. The HTTP protocol and conventions are extremely flexible and robust in overcoming obstacles, even beyond the original design intent of HTTP.

If a customer wanted to access web pages of a site, "www.scofflaw.example.com", and found that the IAP was filtering packets to that site, the user could simply find an HTTP proxy server outside the control of the IAP and "bounce" requests through it. A proxy server performs web browsing requests for a third party. Normally, a web browser sends its requests directly to the desired site. All web browsers can also be configured to use a proxy server. When so configured, each user request is bundled up and sent to the named proxy server. The proxy server

unbundles the request, performs the requested access, and returns the results to the user. The process is analogous to a hotel concierge obtaining theater tickets for a hotel guest. Proxy servers are often used to facilitate IAP or organization security arrangements or to improve performance.

Suppose the proxy server is a host named "proxy.sbwu.edu". As far as router packet filters were concerned, all IP packets would be traveling between the IAP customer and "proxy.sbwu.edu". Since the HTTP proxy host is outside the network facilities directly controlled by the IAP, the fact that packets traveled between "proxy.sbwu.edu" and "scofflaw.example.com" would be completely invisible to the IAP and the IAP's routers.

If a proxy server allows itself to be used to access infringing sites, the proxy server could also be blocked. The list of "renegade" proxy servers could be added to the list of infringing sites, and whatever techniques are used to block direct access to infringing sites could also be used to block access to the listed proxy servers.

Thousands of HTTP proxy servers exist today, both in the U.S. and beyond. Many of those proxy servers are unrestricted with respect to who uses them. New servers come and go every day. In number terms, this activity magnifies the problems described earlier.

Blocking proxy servers also begs the test of reasonableness. Many proxy servers are operated on the very same machines that sites use to host normal web servers. Blocking access to the HTTP proxy server would effectively require blocking access to the entire site. HTTP proxy service would likely only be a minor part of the sites traffic, and within proxy service, relays to infringing sites would be an even smaller percentage.

Would it be possible to look for HTTP proxy requests in packet data? If the IAP could examine proxy requests, then the ultimate destination for the request would be easily seen, and the request could be blocked. Because HTTP is an application-level protocol, all of the data for the request and the response are carried in the payload data in the IP packets. Equipment and software used to move packets in the Internet today examine only the TCP/IP header bytes and leave the payload data unexamined and unaltered (just as a delivery service uses address information without understanding the package contents).

Because packet data does not arrive as a single block the packets can arrive in a different order than they were sent. As a result, some packets may be lost, and only a certain number of packets will be sent before acknowledgments are received for earlier packets, making the job of the computer analyzing the payload data extremely difficult. This computer must gather packets, reassemble payload data in the proper sequence, and then do any application-specific scan. The algorithmic details and performance costs make this solution unfeasible, both in terms of economics and efficiency.

Even if the situation were otherwise, the approach could be easily thwarted by masking the request to make it look like a protocol other than HTTP. Suppose, for instance, a user is still trying to reach "www.scofflaw.example.com", this time using a proxy server. The user has reason to believe, however, that the proxy server is blocked too. The persistent user masks the HTTP proxy request with the Network News Transfer Protocol (NNTP), used for reading netnews on the Internet. Like HTTP, NNTP is a text-based application protocol. A cooperating user and

proxy server would pretend to be performing an NNTP conversation. At some mutually understood point in the conversation, the user's software would send the proxy request. The proxy server would interpret and act on the request, as usual, and return the results to the user.

The NNTP example illustrates two new requirements for IAPs attempting to do the blocking. First, they must constantly be on the lookout for new points at which the conversation turns into a proxy request. This would probably vary from site to site. It would also vary for a given site as more and more IAPs became aware of a given technique and the site switched to new techniques. For example, at one site the technique might be to switch right after seeing a command containing the string "XYZZY". At another site, it might be to switch after 200 bytes had been transmitted.

Second, the IAP must not merely examine the beginning of a data exchange to decide if it is an HTTP proxy request but must monitor the entire conversation. Since more packets must be examined and more patterns must be sought, this increases the cost and performance burden for the IAP.

While the counter measures described above may appear to be the provenance of only a small group of highly sophisticated users, this is really not the case. The know how necessary to evade access controls is widely available; ironically, the Internet itself makes much of this information available. And while those seek to evade controls have a single target, the IAP operates in a one to many environment, with thousands of users devising tens of thousands of new approaches to beat the system. In this scenario, the point of diminishing returns is quickly reached. No approach is fool proof. Rather, as this discussion suggests, once content is released unprotected to the Internet, a pound of prevention is worth an ounce of cure. In attempting to retrofit a solution, the very steps taken to protect digital content make that content less convenient, more expensive and, in the end, less attractive. Even that which is technically feasible becomes economically unreasonable.

Conclusion

Clearly, the solution to Internet copyright lies beyond the internal architecture of the Internet. As this section suggests, effective copyright protection cannot be relegated to the point where content is on the transmission path of the Internet. Instead, the only effective points of control are at the point of transmission and the point of reception. This reality places the responsibility of "wrapping" or otherwise placing digital "identifiers" onto or around valuable intellectual property with the copyright holder and content provider. Protecting content in this manner will result in discouraging infringement "initiators" and provide IAPs with the digital tools that will make it technologically feasible and economically reasonable to deal with unauthorized reproductions. Section Three of this paper explores the technologies which can make a critical difference, giving copyright holders the tools necessary to protect their valuable content.

Section Three

Digital Copyright Protection Technologies

Introduction

"Digital copyright." The phrase itself contains an inherent contradiction. Digital technologies make near perfect reproduction simple and affordable. Copyright laws make various unauthorized forms of

reproduction illegal. Copyright holders want to use the digital technology to deliver their valuable property to a wider audience. But they also want the value of their property preserved in an environment which makes protection difficult. Internet communications companies must attract digital content to be able to grow their own infrastructure investments. But the technology which makes value-added services possible can also be misappropriated to make copyright infringement a definite possibility. Holding information distributors liable for the handling of content over which they have no knowledge and little control, however, throws the entire dynamic of the Internet into serious question. Small wonder the issue is so contentious and often so confusing.

Neither treaties nor legislation have yet to bring balance to the situation. Perhaps such an expectation is unrealistic, at least for the short term. Compared to information technology, law moves at a glacial pace. At the same time, content and Internet access and service providers need to work together cooperatively to establish a safe environment for content distribution and a worthwhile investment in the infrastructure. The Internet communications community is working to develop technology tools which empower copyright holders to protect their content at the level they believe is required.

The latest technologies which content providers can utilize – at various levels – to protect and allow access providers to identify their works include digital envelopes, encrypted signal streams, software metering methods and tools, digital watermarks, authentication devices, digital signatures and copyright management tools. Business practices are also beginning to be established that will further protect copyrighted works placed in the digital environment. For example, a copyright holder fearing rampant unauthorized copying of content on its web site may configure its content server to selectively serve up the content only to third party proxy servers that agree to certain copying rules and restrictions.

ITAA has begun to assemble a list of companies and their technologies which can facilitate copyright protection in the digital medium. While this summary is as complete as possible at the time of printing, it is certainly not exhaustive. Additional technologies exist, are continually being developed, and will be placed on the ITAA Internet web site as they come to the Association's attention (<http://www.itaa.org>). ITAA makes no claims as to the comprehensiveness of this collection, nor can ITAA make any claims as to the validity of the claims made by the providers of these technologies. All information provided is summarized and condensed from company press releases and responses to requests for information. It is here as a representative sampling of what content providers can utilize so that they can take advantage of the digital medium without fear of piracy, exploitation, and unauthorized copying.

Some of these new protection tools provide varying degrees of security, allow the payment of royalties, and/or track violations so that the true offenders – the "initiators" of unauthorized reproductions – can be dealt with within the framework of the current and enforceable copyright laws. As with most emerging technologies, there is a varying degree of protection and efficiency among technologies available for copyright protection. The array of options allows content owners to select the level of protection they feel most accurately represents their need for protection instead of being shoe-horned into a one-size-fits-all legislative category. The choice is left in the hands of those in a position most able to make the correct decision.

The "debate" as it were should not be "who is responsible," but rather, how

to best work together to protect this valuable medium and the content which will be distributed on it. The Internet access and service providers and the copyright holders and content providers are allies, not enemies. As with any successful community, the citizens of this digital community must work together to efficiently, economically, profitably deliver to the legitimate end-user, enhanced and copyright protected valuable content.

Protection rests on three principles: (1) enforcement of copyright laws; (2) education of end-users and customers; and (3) embracing protection-empowering technologies at the beginning of the distribution cycle. Cross-industry cooperation and self-regulation will enhance digital copyright protection and spread the value of Internet and the World Wide Web to a wider audience.

Compendium of Digital Copyright Protection Technologies

Name of Product: Argent

Name of Company: DICE Company

Type of Protection: Digital Watermark

Medium Protected: Digital Audio and Video

Summary

Argent is a system that integrates a hidden and indelible "digital watermark" within a digitized image, video recording, or audio recording. This watermark can then be read by computer to reveal information such as to whom the copy was legally sold to, the creator, and payment information.

Contact Person: Marc Moskowitz

The DICE Company

PO Box 60471

Palo Alto, CA 94306-0471

www.xynet.com/argent/

Name of Product: Cryptolope Containers

Name of Company: IBM

Type of Protection: Secure Information Packaging

Medium Protected: Multiple formats, including ASCII text, HTML, JPEG, etc.

Summary

A secure container architecture for packaging and distributing information content and properties. Cryptolope is short for cryptographic envelope. The Cryptolope container holds an encrypted version of a document (which may contain ASCII text, HTML, image, video, etc.) as well as rules for determining permissions specified by the content provider. The

Cryptolope container also holds control information that describes the document contents such as an abstract, price, and restrictions or terms and conditions on the use of the document. This control information is available without decrypting the actual document contents.

Contact Person: Mike King

mikeking@gemini.ibm.com

IBM

Route 100

Somers, New York 10589

www.infomarket.ibm.com

Name of Product PICS

Name of Company W3C

Type of Protection Digital Headers

Medium Protected Every type of content represented in HTML

Summary

PICS is an infrastructure for associating labels with Internet content. It was originally designed to help parents and teachers control what children access on the Internet, but it also facilitates other uses for labels, including code signing, privacy, and intellectual property rights management.

Contact: www.w3.org

• Jim Miller (jmiller@w3.org)

• Paul Resnick (presnick@research.att.com)

• Danny Weitzner (djw@cdt.org)

Name of Product MusiCode

Name of Company ARIS Technologies, Inc.

Type of Protection Digital Watermark

Medium Protected Music (or video), independent of the media.

Summary

MusiCode is a digital watermarking process which allows record companies to insert inaudible copyright information within audio or video. This watermark can be used to track royalties, deter copying, and even prevent copying of digital or analog music. MusiCode is an enabling technology which makes protected online music distribution possible.

Contact Person: Richard Gastwirt, Director of Marketing

ARIS Technologies, Inc.

51 Middlesex Street
North Chelmsford, MA 01863
phone: (508) 251-4844
email: rdg@aristech.com

Name of Product PictureMarc

Name of Company Digimarc

Type of Protection Digital Watermark

Medium Protected Images

Summary

PictureMarc embeds an imperceptible digital watermark within an image. The watermark carries copyright information and links to the image creator, enabling copyright communication, authorship attribution and electronic commerce. Coupled with Digimarc's aggressive distribution strategy, PictureMarc promises to yield a viable solution to the long-standing problem of how to communicate copyright in a digital setting. A Digimarc watermark is durable, able to survive across file formats and most transformations of the image such as copying and editing, and can be read even when the image is cropped. The watermark is embedded digitally within the image, remaining a part of the image even when printed, and can be read by scanning the printed image into a computer. This durability ensures that the watermark stays with the image wherever it may travel.

Contact Digimarc Corporation

521 SW 11th Avenue, Suite # 200

Portland, OR 972051

Phone: (503) 223-0118 fax: (503) 223-6015

info@digimarc.com www.digimarc.com

Name of Product SCAM (Stanford Copy Analysis Mechanism)

Name of Company Dept. of Computer Science, Stanford University

Type of Protection Registration and Query Mechanism

Medium Protected Text documents and images (and pretty much all forms of digital media)

Summary

Authors and publishers register their documents and digital objects into the SCAM server through a friendly web, Java, or email interface. The SCAM server then searches web and FTP sites on the Internet, and Usenet newsgroups in a continual fashion for copies and notifies the author of the registered object. In the case of text documents, it also identifies sites with partial copies (e.g.: a few chapters, paragraphs, etc.) of the registered documents. SCAM is a research prototype constantly being improved

upon for added functionality and improved performance.

Contact Person: Marayan Shivakumar & Hector Garcia-Molina

Department of Computer Science, Wing 4A, Gates Hall

Stanford University

Stanford, CA 94305

<http://www.dlib.org/dlib/november95/scam/11shivakumar.html>

Name of Product (Patent Pending)

Name of Company Mitretek

Type of Protection Digital Access Control

Medium Protected Any Digital Medium

Summary

The system would enable the owner of intellectual property, through an electronic license, to accord users various degrees of access and/or ability to copy the information. Specifically, a user would purchase a license that would explicitly control "read" access to various portions of the IP, "print" options (perhaps forcing a "watermark" on each page of output), and "copy" options (generally not permitting wholesale copying, but perhaps allowing the copying of a paragraph or individual images). When copies are permitted, the resulting "derivative works" are themselves controlled by an electronic license (that might be issued by the owner of the original work!) in the same fashion as the original. The invention is equally applicable to software and to entertainment (as well as any other form of digital information) and would allow complete interoperability among all data types and uses.

Contact Person: Paul Schneck - schneck@mitretek.org

Director of Information Systems

Mitretek Systems

7525 Colshire Drive

McLean, VA 22102

ph (703) 610-2305 fax: (703) 610-1805

Name of Product Digital Property Rights Language (DPRL)

Name of Company Xerox

Type of Protection Specification of rules governing the use and pricing of content

Medium Protected Multiple formats, including ASCII text, HTML, JPEG, etc.

Summary

Xerox's DPRL technology provides the language needed by content providers to specifically designate what actions are sanctioned by end users with regard to specific intellectual property. In combination, these two technologies will afford intellectual property rights holders the means for enhancing their control over the use of their content within a network environment.

Contact Person: Mark Stefk - stefik@parc.xerox.com

Name of Product SoftLock

Name of Company SoftLock Services, Inc.

Type of Protection Piracy protection

Medium Protected all digital distribution media

Summary

With the integration of SoftLock's patented technology and password vending services, software and documents can be sold as easily as they are created. SoftLock's technology allows authors and publishers to lock files and functions so that they can be unlocked and purchased in minutes from our automated password vending systems. Now you can distribute software or files freely, knowing that only paying customers will be able to use them. Customers access the files thought the purchase of a password which is available 24 hours a day at 1-800 SOFTLOCK and on the Web at www.softlock.com. And you can encourage copying because products automatically re-lock and invite another purchase when moved from one machine to another.

Contact Person: Martin Presberg, Director of Client Services

SoftLock Services, Inc.

36 Brunswick St.

Rochester, NY 14607

(716) 242-0348 [http://www.softlock.com/info@softlock.com](mailto:info@softlock.com)

Name of Product ReadMarc™

Name of Company Digimarc Corporation

Type of Protection Digital watermark reader

Medium Protected Watermarked still images

Summary

ReadMarc(TM) is a stand-alone digital watermark reader for Windows and Macintosh that is available free to download off the Digimarc(TM) website at www.digimarc.com. ReadMarc is the latest addition to Digimarc's PictureMarc(TM) family of digital watermarking products and brings the benefits of Digimarc's technology to anyone who views, copies or downloads digital images. ReadMarc complements the integration of PictureMarc in tools such as Adobe Photoshop(R) 4.0 and CorelDRAW(TM)7 by seamlessly providing watermark read capabilities within the user's desktop environment. For example, ReadMarc

continuously monitors the Window's clipboard so that when an image is copied onto the clipboard, ReadMarc automatically performs a quick detect and notifies the user if a Digimarc watermark is present. From there, the user can read the watermark and obtain detailed information about the image creator through MarcCentre(TM), Digimarc's online locator service. This automatic detection feature is integral to Digimarc's overall strategy of allowing image creators to communicate directly with image consumers. In addition, ReadMarc supports Macintosh, Windows 95 and Windows NT operating system specific features such as drag and drop and right-click menus.

Contact:

Digimarc Corporation

521 SW 11th Avenue, Suite # 200

Portland, Oregon 97205

ph: 1 (800) DIGIMARC, ph: (503) 223-0118, fx: (503) 223-6015

e-mail: info@digimarc.com WWW: <http://www.digimarc.com>

Name of Product InterTrust Commerce Architecture, DigiBox container

Name of Company InterTrust Technologies Corporation

Type of Protection Secure Information Packaging

Medium Protected All digital information on any electronic media, including networks and CD-ROM

Summary

The InterTrust Commerce Architecture™ is a digital rights management system that persistently protects the rights of content creators and distributors on the Internet, online services, enterprise networks, and storage media such as CD-ROM. It allows anyone to control access to and use of digital information by putting it into a container called a DigiBox™ along with business rules that govern the use of the contents. Content owners can control, for example, who can access the content, who can modify it, how it can be used (view, print, excerpt, etc.), how much it costs, and whether recipients are allowed to pass along the protected content to others. Even after a piece of content has been paid for, it continues to be subject to the associated rules and cannot be taken from the container, preventing illegal copying. The InterTrust architecture supports multiparty chains. Distributors and other value chain members can modify the DigiBox contents (such as pricing) subject to permissions set by prior members in the chain. Payment and usage information generated as a result of content access is also packaged in DigiBox containers and is sent from consumers to clearinghouses. Clearinghouses process this information and pass it on to creators and distributors. DigiBox containers - it must be noted - can also support the secure communication of private information, such as Electronic Data Interchange, email, and electronic financial transactions. The InterTrust Commerce Architecture is being deployed through InterTrust's partners, which include SOFTBANK Net Solutions and Mitsubishi Corporation.

Contact:

InterTrust Technologies Corporation**460 Oakmead Parkway****Sunnyvale, CA 94086****Tel: 408.222.6100 Fax: 408.222.6144****E-mail: info@intertrust.com <http://www.intertrust.com>****Name of Product WebArmor****Name of Company WebArmor****Type of Protection Secure Web Archiving****Medium Protected World Wide Web Sites****Summary**

WebArmor is software that facilitates copyright protection of your web site. WebArmor archives your web site and affixes an authoritative, encrypted time-date stamp and content signature. You can then show, in court if necessary, what your web site looked like at a particular instant in time. If you suspect that someone has plagiarized your HTML or stolen some of your online artwork, a WebArmor-archived copy of your site can PROVE that "you had it first" on your site.

Contact:**WebArmor****Phone: (412) 683-6210 Fax: (412) 683-6415****Email: webmaster@webarmor.com <http://www.webarmor.com>****Name of Product CCC Online****Name of Company Copyright Clearance Center****Type of Protection Digital Rights Clearinghouse****Medium Protected All media represented****Summary**

The Copyright Clearance Center (CCC) was established by authors, publishers and users as the not-for-profit Reproduction Rights Organization (RRO) for the United States. CCC operates collective licensing systems that facilitate compliance with the copyright law and promote the Constitutional purposes of copyright, namely progress and creativity in the arts and sciences. CCC's mission is: 1. to act as an agent for domestic/foreign authors and publishers by providing them with the efficiencies of collective services through equitable collection and distribution of royalties for photocopying and electronic uses of their copyrighted printed works; 2. to provide all types of users with an efficient single source for licensed access to as broad a repertory of copyrighted works as possible; and 3. to continue development of collective licensing systems that meet the challenges of emerging information technologies.

Contact:**Copyright Clearance Center****222 Rosewood Drive****Danvers, MA 01923****Tel: 508-750-8400 / Fax: 508-750-4744 <http://www.copyright.com>****Name of Product Flickering Screen****Name of Company Bellcore****Type of Protection Prevents On line Piracy****Medium Protected All online content****Summary**

Bellcore's Flickering Screen technology gives publishers another tool to help prevent on-line piracy of their materials. Flickering Screen relies on the perceptual properties of the human eye, using two unreadable images interleaved quickly to create a readable image that cannot be screen dumped since the readability depends on averaging in the human eye. While other protection methods might allow users to access a publisher's material only through proprietary software that does not allow downloading, these methods do not prevent users from "screen scraping," or taking "screen dumps," of the images that actually appear on a screen. Bellcore's Flickering Screen technology is a program that displays text on a screen in such a way that users can read it but cannot capture it through a screen dump. The program flickers the text with an admixture of gray noise. The human eye sorts out the letters and reads them, not paying close attention to the gray background. However, any screen dump captures the item at one instant, including the noise. The text is also scrolled up and down slowly, which again the human eye can track but which would frustrate a program trying to average out the flickering.

Contact Person: Trisha Rimo**Bellcore****2101 L Street, NW, Suite 600****Washington, DC 20037 USA****Voice: (202) 776-5466 - Email: trimo@notes.cc.bellcore.com****Name of Product @ttribute™****Name of Company NetRights, LLC****Type of Protection Copyright information linked to digital work**

Medium Protected @ttribute links copyright information to many different digital file formats including but not limited to audio, video, images, graphics, and text.

Summary

@ttribute is a compelling new technology that energizes commerce between the owners and creators of digital content. @ttribute was created by NetRights in response to the need for a uniform, timely, and persistent means of identifying digital content in the networked environment. Currently very few media types provide for any form of identification within their respective file formats. Fewer do it in a way that is flexible, allowing the owner to choose what information should be presented and how. And none do it in a way that allows the content element to provide its own interfaces and facilitate communications with its "home" (owner, creator, rights administrator or some other entity), regardless of its context. There is no other solution currently available that provides what @ttribute provides to enhance attribution to identify owner, creative contributors, and performance clearances of digital work; allow open access for browsing and reviewing work using industry-standard object technology; interface directly with creativity tools currently used; and facilitate automated and negotiated licensing terms between the owner/creator and a developer/publisher. These features are part of a comprehensive, powerful and unique system.

Contact Person: Mary Gavin, Product Marketing Manager

NetRights, LLC

One Court Street, Suite # 370

Lebanon NH 03766

phone (603) 448-3355, fax (603) 448-1580

<http://www.netrights.com>mary.gavin@netrights.com

Name of Product Clickshare Access and Payment System

Name of Company Clickshare

Type of Protection Digital Payment and Access Control

Medium Protected All online content

Summary

The Clickshare system removes one of the biggest barriers to the further evolution of the Internet by giving users simple access to a free market of information -- while sparing them the inconvenience of multiple passwords, registrations and credit relationships. The Clickshare open standard for micro-transaction settlements gives publishers an economic incentive to cooperate in exchanging both users and information through guaranteed royalties and referral commissions. Clickshare offers marketers and advertisers an improved way to measure Web traffic across multiple unrelated servers, correlated to demographic information (if users wish to make it available).

Contact:

Clickshare Corp.

Seventy Five Water St.,

P.O. Box 367

Williamstown, MA 01267-0367 USA

Voice: (413) 458-8001 / Fax: (413) 458-8002

Email: mail@newshare.com

US Patent #6,078,664 Z-transform implementation of digital watermarks

Abstract (US Patent #6,078,664 Z-transform implementation of digital watermarks)

Z-transform calculations may be used to encode (and/or decode) carrier signal independent data (e.g., digital watermarks) to a digital sample stream. Deterministic and non-deterministic components of a digital sample stream signal may be analyzed for the purposes of encoding carrier signal independent data to the digital sample stream. The carrier signal independent data may be encoded in a manner such that it is restricted or concentrated primarily in the non-deterministic signal components of the carrier signal. The signal components can include a discrete series of digital samples and/or a discreet series of carrier frequency sub-bands of the carrier signal. Z-transform calculations may be used to measure a desirability of particular locations and a sample stream in which to encode the carrier signal independent data.

US Patent #5,905,800 Method and system for digital watermarking

Abstract (US Patent #5,905,800 Method and system for digital watermarking)

A method for applying a digital watermark to a content signal is disclosed. In accordance with such a method, a watermarking key is identified. The watermarking key includes a binary sequence and information describing application of that binary sequence to the content signal. The digital watermark is then encoded within the content signal at one or more locations determined by the watermarking key.

US Patent #5,889,868 Optimization methods for the insertion, protection, and detection of digital watermarks in digitized data

Abstract (US Patent #5,889,868 Optimization methods for the insertion, protection, and detection of digital watermarks in digitized data)

The implementations of digital watermarks can be optimally suited to particular transmission, distribution and storage mediums given the nature of digitally-sampled audio, video and other multimedia works. Watermark application parameters can be adapted to the individual characteristics of a given digital sample stream. Watermark information can be either carried in individual samples or in relationships between multiple samples, such as in a waveform shape. More optimal models may be obtained to design watermark systems that are tamper-resistant given the number and breadth of existent digitized sample options with different frequency and time components. The highest quality of a given content signal may be maintained as it is mastered, with the watermark suitably hidden, taking into account usage of digital filters and error correction. The quality of the underlying content signals can be used to identify and highlight advantageous locations for the insertion of digital watermarks. The watermark is integrated as closely as possible to the content signal, at a maximum level to force degradation of the content signal when attempts are made to remove the watermarks.

US Patent #5,822,432 Method for human-assisted random key generation and application for digital watermark system

Abstract (US Patent #5,822,432 Method for human-assisted random key generation and application for digital watermark system)

A method for the human-assisted generation and application of pseudo-random keys for the purpose of encoding and decoding digital watermarks to and from a digitized data stream. A pseudo-random key and key application "envelope" are generated and stored using guideline parameters input by a human

engineer interacting with a graphical representation of the digitized data stream. Key "envelope" information is permanently associated with the pseudo-random binary string comprising the key. Key and "envelope" information are then applied in a digital watermark system to the encoding and decoding of digital watermarks. The invention includes improvements to the methods of encoding and decoding digital watermarks. Improvements are: separation of the encoder from the decoder, increased information capacity relative to spread spectrum methods, destruction of content resulting from attempts to erase watermarks, detection of presence of watermarks without ability to access watermark information, multi-channel watermark capability, use of various classes of keys for watermark access control, support for alternative encoding, decoding, or other component algorithms, use of digital notary to authenticate and time stamp watermark certificates.

US Patent #5,745,569 Method for stega-cipher protection of computer code

Abstract (US Patent #5,745,569 Method for stega-cipher protection of computer code)

A method for protecting computer code copyrights by encoding the code into a data resource with a digital watermark. The digital watermark contains licensing information interwoven with essential code resources encoded into data resources. The result is that while an application program can be copied in an uninhibited manner, only the licensed user having the license code can access essential code resources to operate the program and any descendant copies bear the required license code.

US Patent #5,687,236 Steganographic method and device

Abstract (US Patent #5,687,236 Steganographic method and device)

An apparatus and method for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.

US Patent #5,613,004 Steganographic method and device

Abstract (US Patent #5,613,004 Steganographic method and device)

An apparatus and method for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.

US Patent #5,539,735 Digital information commodities exchange

Abstract (US Patent #5,539,735 Digital information commodities exchange)

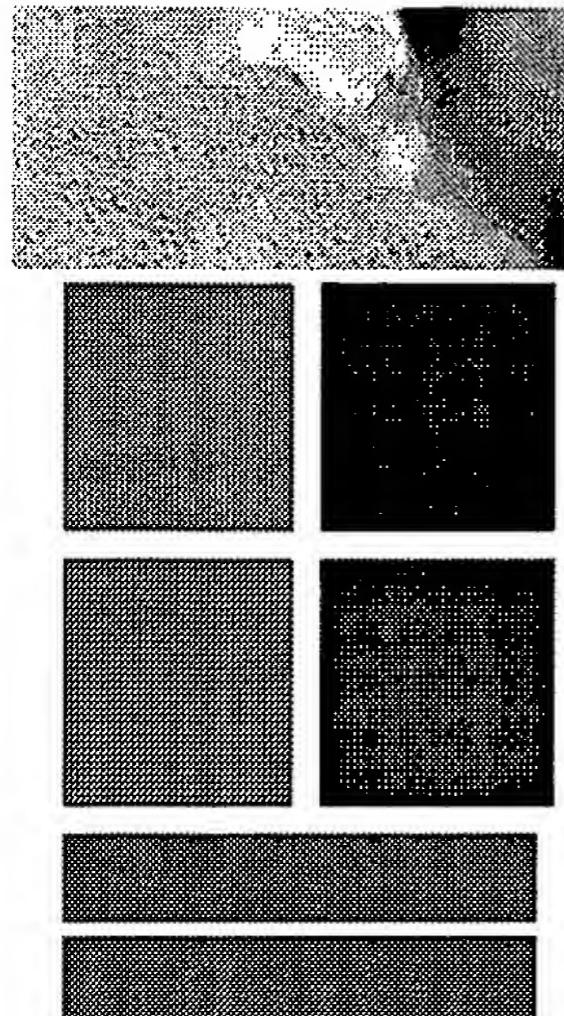
A system for the exchange of digital information packets includes an exchange with connectors to allow

modular expandable units to connect to the exchange over transmission media. The modular expandable units send digital information packets from one to another over the exchange in response to requests for these digital information packets. The exchange allows for billing and other administrative functions.

US Patent #5,428,606 Digital information commodities exchange

Abstract (US Patent #5,428,606 Digital information commodities exchange)

A system for the exchange of digital information packets includes an exchange with connectors to allow modular expandable units to connect to the exchange over transmission media. The modular expandable units send digital information packets from one to another over the exchange in response to requests for these digital information packets. The exchange allows for billing and other administrative functions.



BLUE SPIKE

ART COMMERCE SCIENCE & TECHNOLOGY GIOVANNI ABOUT BLUE SPIKE HOME

Genesis Myth

It is the simplest of observations that often provokes the most profound innovations. For Blue Spike, Inc. the inciting incident that launched the company was the theft and reclamation of the founder's personal property. Founder Scott Moskowitz thought he had lost a ruler he was using for his graphic design class at a North Miami Beach junior high school. He had, however, taken the precaution of marking one edge of the ruler with indelible red ink to assure that his title to this instrument would be obvious to all, the nascent business mind at work even then.

Moskowitz recovered the ruler when a friend, the hawk-eyed Michelle Honig, spied it in the possession of the would-be thief, another student at Moskowitz's school. The perpetrator had attempted to obscure the red signature by scribbling over it in pencil - but enough of it remained visible to clue righteous Michelle onto its rightful owner. Michelle confronted the thief, condemned his perfidy and reclaimed the ruler for her classmate.

That event taught founder Scott Moskowitz an important lesson that he sums up to this day with the maxim, "People lie, cheat and steal." Before he made his way to college at Penn, well wise to the ways of a world populated by the light-fingered and the forgetful, Moskowitz refined his primitive proprietorship-assertion scheme to protect a collection of more than a hundred CDs he was bringing with him to the school.

Moskowitz took a fine pen knife and carefully etched his initials - SM or SAM - into the inner ring of the discs and at the edge of the jewel cases for all his music CDs. It was small, but visible enough so that it could be located by Moskowitz when he wanted to reclaim the misplaced CD in the hurly-burly of dorm life.

"I wouldn't tell everyone what I did but whenever I saw a disk in a dorm hall or a friend's place and if I saw my initials on a CD, I would take it back. I basically signed my property in a way that only I could tell my signature was there. It wasn't a strong secret - but it would be enough to tell me if something was mine," Moskowitz says.

Digital watermarking & steganography

Companies & products

- AutoKey ([Cognicity](#), U.S.A.) is a copyright marking system for audio. The team includes Mitchel Swanson, Bin Zhu and [Ahmed Tewfik](#).
- Copysight ([Intellectual Protocols2](#), Louisiana, U.S.A.) is a Java-based service that tries to assert and safeguard the intellectual property rights of their customers against Internet pirates.
- [Cryptotope](#) is IBM's electronic copyrights management system.
- [DCT - Digital Copyright Technologies](#) is a Switzerland based start-up using technologies from É.P.F.L. and University of Geneva.
- [DICE Company](#) (Tokyo, Japan) holds various US patents on watermarking: [#5428606](#), [#5539735](#), [#5613004](#) and [#5687236](#).
- [Digimarc Plugins](#) (formerly PictureMarc) ([Digimarc](#), Portland, Oregon, U.S.A.) is a marking system for images based on pattern block encoding. It is available as an Adobe Photo Shop plug-in. Its companion [MarcSpider™](#) is supposed to crawl through the Web to locate Digimarc watermarked images. Related US patents: [#5636292](#) and [#5710834](#)
- E-DNA Solana Technology Development Corp. has developed a watermark technique for audio called Electronic DNA. Related US patents: [#5687191](#), [#5719937](#) and [#5822360](#).
- [EIKONAmark](#) ([Alpha Tec Ltd](#), Greece)
- [FlashPix](#) (New Mexico Software, Albuquerque, New-Mexico, U.S.A.) provides an imaging architecture. This is a partner of [Signum Technologies](#).
- [IBM](#) - Watermarks: Protecting the image ([Howard Sachar](#), IBM T. J. Watson Research Center). Visible ([Vatican Library Project](#) -- see [some samples](#)) and invisible watermarks (DCT based techniques). Other project on [Digital Libraries](#) and [data hiding](#).
[Can Invisible Watermarks Resolve Rightful Ownerships?](#)

- ICE & VEC (CRL), Middlesex, United Kingdom) are audio watermarking and image watermarking hardware respectively.
- Giovanni (Bluespike) is a marking system for still images and audio. It is based on DICE's patents.
- LicensIt (NetRights, Lebanon, New Hampshire, U.S.A.) provides a plug-in for Adobe Photoshop. Contact: John S. Erickson <john.erickson@netrights.com> -- One Court Street, Suite 370 Lebanon, NH 03766, U.S.A.
- Musicode (ARIS Technologies, Cambridge, Massachusetts, U.S.A.): an obscure marking system for audio. In January 1998, ARIS signed an agreement with SESAC, which is now the first user of Musicode. Musicode claims to deliver indelible, inaudible copyright protection, identifying proof of ownership, proof of copyright violation and unauthorized copy prevention of music. Related international patent: WO 98/53565
- OwnerMark(Signafy, Inc., Princeton, New Jersey, U.S.A.). Signafy is a venture startup established by NEC to market digital watermarking security solutions for multimedia and DVD. The technique is based on DCT or FFT with "secure spread spectrum" is explained in A Secure, Robust Watermark for Multimedia, a paper presented at the First International Workshop on Information Hiding. Related US patent: #5848155.
- ImageSafe (Collin Mummary, EquitySoft, England), a java based tool to protect images. Each image is incorporated into the java code and does not appear into the cache of the browser.
- Scarlet (Aliroo, Kefar-Sava, Israel) is a software package for copyright protected trading of digital images and sound files. It enables a potential buyer to experiment with the images in full resolution, and the publisher expect that his images will not be used without the purchase of a license.
- SecureSuite (Fotonation, California, USA). [Patents]
- SureSign (Signum Technologies, Oxford, England) embeds digital fingerprints into binary images. The software is in fact a plug-in for Adobe Photoshop. The watermark is embedded in the spatial domain using a technique similar to direct sequence spread

spectrum.

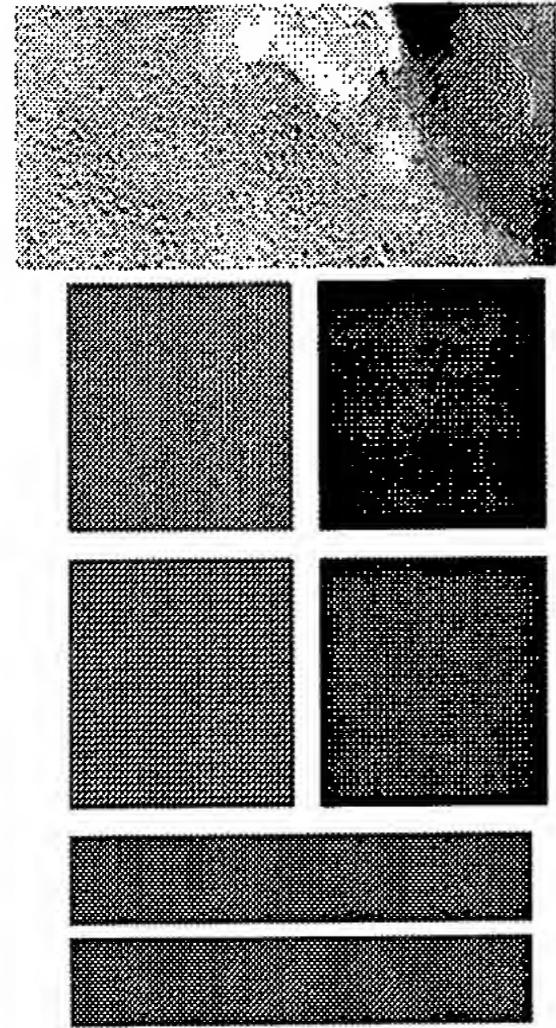
- SysCoP (Fraunhofer Institute for Computer Graphics, Darmstadt, Germany / MediaSec Technologies LLC, Providence, Rhode Island, U.S.A.) embeds digital watermarks in pictures and video. It proposes a WWW service for copyright management. The technique is presented in Towards Robust and Hidden Image Copyright Labeling
- WaveMeter (Wave Systems Corp. Lee, Massachusetts, U.S.A.) is an information metering system based on a proprietary semiconductor chip. The Wave system try to guarantee owners of electronic content accurate information on how their customers interact with the content (usage, purchasing, quantity, timing, frequency and spending).

Other related sites

- AT&T - security software.
- AudioSoft (France).
- MPEG-4 Intellectual Property Management & Protection (Fraunhofer MMP, Germany).
- Macrovision Corp.
- MediaSec Technologies LLC.
- Microtrace, Inc. (Minneapolis, Minnesota, U.S.A.).
- r³ security engineering ag (Switzerland).



Copyright © 1997-2000 by Fabien A. P. Petitcolas, Computer Laboratory, University of Cambridge



BLUE SPIKE

[ART](#) ... [COMMERCE](#) ... [SCIENCE & TECHNOLOGY](#) ... [GIOVANNI](#) ... [ABOUT BLUE SPIKE](#) ... [HOME](#)

Blue Spike's Technology Partners

As purveyors of vital security infrastructure technologies for electronic commerce, Blue Spike, Inc. has been attracting the interests of a good many industrial peers. The company finds itself at the intersection of the information security disciplines, the digital signals processing arts and the exciting new world of online music distribution. Over the years, Blue Spike and its partners from those fields have cross-licensed their technologies, allowing Blue Spike's developers to integrate best-of-breed technologies into its own product suites. Stay tuned for new announcements about further licensing deals, some of which will deliver product and service suites that the company is developing.

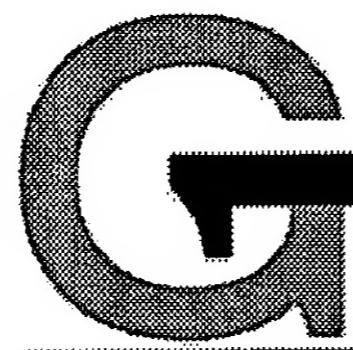
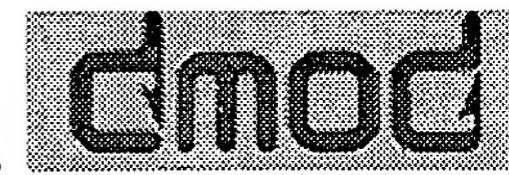
This January, Blue Spike integrated Lucent's Enhanced Perceptual Audio Coder (ePAC) into the company's Trusted Transaction Server, a server product that offers an "end-to-end" solution to distributors of music. The TTS organizes all of the components required for piracy-proof music products. NTRU's cryptographic system provides the delivery wrapper. Blue Spike's digital watermarking embeds persistent protection - and Lucent lends its ePAC codec for gorgeous audio quality.

 **Lucent Technologies**
Bell Labs Innovations



NTRU Cryptosystems are pushing the envelope of cryptographic speed with their cryptographic systems that have the computational ability to keep up with today's online consumer transaction loads. For Blue Spike's Trusted Transaction Server (TTS), the company integrated NTRU's blazing fast cryptosystem to provide the TTS' Download Package (DLP). Instead of wrapping the content in a single container using one key like other schemes, NTRU's method encrypts every few seconds of data with a different key, effecting an incredibly strong security system by maximizing the number of cracks that would have to be performed to acquire an entire song.

Online music distributor DMOD is building its vision of a ubiquitous platform allowing access to digital goods from content providers, distributors and media portals through a digital distribution system. To fulfill that dream, DMOD turned to Blue Spike to deliver digital watermarking technologies to secure the copyrights of recorded music in its systems. The DMOD system provides a dual watermark: the first is a copyright watermark, while the second watermark is performed as part of the download request and is applied using the "on-the-fly" capabilities of the DMOD server.

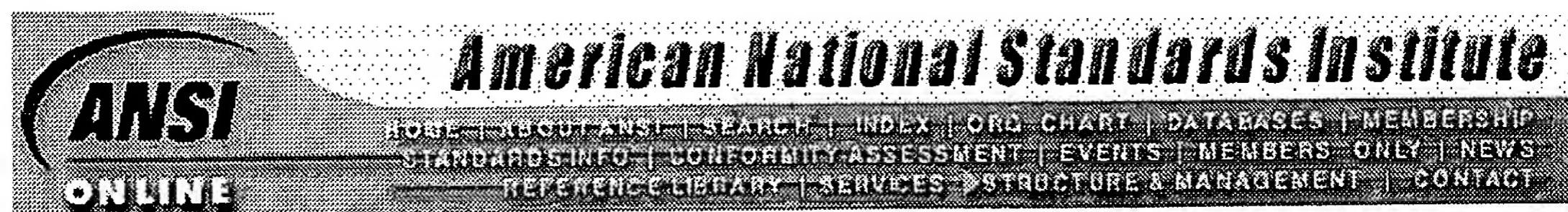


GenuOne and Blue Spike inked a cross-marketing agreement this year with an eye to co-developing service suites. The mutual interests were quite clear. Blue Spike's watermarking technologies can be deployed to authenticate most any content on a Web page, effectively providing a credentializing system that can be used to assure a Web page's authenticity. GenuOne, one of the leading developers of online brand-continuity servers, immediately saw the potential for deflecting page-jacking hacks and for developing a whole new class of certification scheme to tip off consumers to online marketers of gray-market and counterfeit goods.



[EMAIL CONTACT](#)

Copyright © 2000 Blue Spike, Inc. All rights reserved.
Send comments and suggestions to webmaster@bluespike.com



Information Infrastructure Standards Panel

[What's New](#)
[Site Index](#)
[Upcoming Meeting Info](#) ◀
[Mission](#)
[Participant Information](#)
[Working Groups](#)
[Standards Needs Information](#)
[Documents](#)
[News Releases](#)
[1998 Meeting Calendar](#)
[Information Infrastructure Links](#)
[Email Lists](#)
[Staff Contacts](#)
[The Information Infrastructure Report](#)

 [IISP Home](#)

MARCH 12-13, 1998 - MEETING INFORMATION: SCOTT MOSKOWITZ, BLUE SPIKE, INC.

Proposed Title for Presentation: Ownership Issues and Digital Watermark Technology

Speaker Name: Scott Moskowitz
Title: President & CEO
Company: Blue Spike, Inc.
Address: 16711 Collins Avenue, #2505
City, State, Zip: Miami, Florida 33160
Country: USA
Phone: (800) 381-8344
E-mail: scott@bluespike.com
Web Site: <http://www.bluespike.com/>

Presentation Overview

In practical application, "digital watermarks" offer rightsholders a unique opportunity to level the security playing field with their technology counterparts. The vast majority of watermarking systems suffer from faulty implementation and the requirement of an original master for subsequent recovery of watermark information. More cryptographically sound systems are unique in "tamperproofing" media content by limiting access to the watermarks to those with authorized "keys", essentially ciphered maps of the embedded information. A pre-encoding step of performing a secure one way hash makes the key unique. "Watermark key" authentication checks by third parties can be encouraged to create an open, tiered security environment with benefits already evident in existing public-key cryptosystems. The widespread emphasis on embedding cryptographic data versus a cryptographic means for embedding data, offers rightsholders a more efficient approach to establish ownership over copies of content.

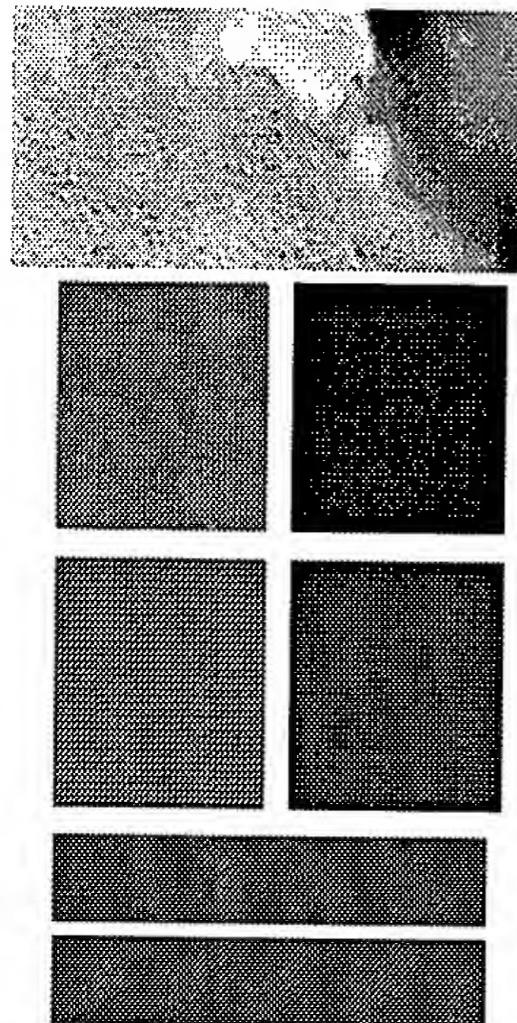
Speaker Background

Scott Moskowitz, president of Blue Spike, Inc., is active in the development of means for the exchange of media over heterogeneous electronic networks including the protection of rights in digitized content. He is the inventor of the Company's innovative digital watermarking and copy restriction technology which includes seven US patents. Mr. Moskowitz also maintains an active media distribution business with exports to Japan.

Company Background

Blue Spike, Inc. is the developer of the Giovanni™ media security system, including applications for digital watermarking, integrating rights, ownership and licensing information into digitized media such as audio, still images and video, and copy restriction software for media works. The Giovanni software suite enables third party arbitration without key or master copy escrow and can be used to prevent unauthorized copying of content. Seven patents cover this innovative approach to tamperproofing media content as well as increasing efficiency in the exchange of such content.

◀ [Return to Presentations List](#)



BLUE SPIKE

[ART](#) • [COMMERCE](#) • [SCIENCE & TECHNOLOGY](#) • [GIOVANNI](#) • [ABOUT BLUE SPIKE](#)

Innovations in Digital Copyright Protection

For those who create, produce, distribute, promote, package and consume digital artwork and music, digital distribution need no longer be tantamount to surrendering your treasures to information highway bandits. With Blue Spike's watermarking technologies, your content can all but phone home. Explore the power of securing electronic content through digital watermarking in the following site segments:

Art

Come see the show at Blue Spike's Future Think Studio, a gallery and a laboratory in which digital art is at last indelibly signed by the artist. And get the inside dope on Metallica's struggle with online piracy.

[\[More\]](#)

Commerce

Online commerce lurches forward in a terrifyingly haphazard and inordinate fashion. Today "e-commerce" might as well stand for "entropy commerce." On the way are the e-labels, e-tags, e-money, e-receipts and e-boxes that will automate online business functions.

[\[More\]](#)

Science & Technology

For users of our Giovanni watermarking system, copyright security is a point-and-click affair. Beneath Giovanni's elegant interface, however, lie intricate orchestrations of psycho-acoustic modeling techniques and the mathematics of cryptography. [\[More\]](#)

Giovanni

Giovanni digital watermarking systems give creators and distributors penetrating control over their digital properties - and they can enable online distribution schemes otherwise unthinkable without prohibitively complex technologies. [\[More\]](#)

About Blue Spike

Look in here for more about our company, its technologies, its intellectual and business provenance, its philosophies, its management team and the exciting news it is generating. [\[More\]](#)

Manifesto: So This is Convergence?

Blue Spike's founder considers the consequences of virtually unlimited distribution capacity being set upon the world today through the Internet - and the role of digital watermarking in bringing technical, legal and commercial order to this penetrating new medium.

Download it here in PDF format: [\[More\]](#)